TECHNISCHE UNIVERSITÄT
CAROLO-WILHELMINA
ZU BRAUNSCHWEIG

UNIVERSITÄTSBIBLIOTHEK
BRAUNSCHWEIG

Grundbegriffe der Galoiskohomologie

Hans Opolka

Braunschweig : Inst. Für Analysis und Algebra, 2010

Elektronisch veröffentlicht am: 19.03.2010

http://www.digibib.tu-bs.de/?docid=00032723

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

GRUNDBEGRIFFE DER GALOISKOHOMOLOGIE

H. Opolka
TU Braunscheig
Institut für Analysis und Algebra
Pockelsstrasse 14
D - 38106 Braunschweig

e-mail: h.opolka@tu-bs.de

Inhaltsverzeichnis

Einleitung

Gegeben sei ein Körper k. Ein wesentliches Anliegen der Galoiskohomologie ist die Klassifikation gewisser über k definierter kategorieller Objekte bis auf k-Isomorphie, und zwar unter der Voraussetzung, daß deren Klassifikation bis auf K-Isomorphie über einer hinreichend großen Galoiserweiterung K/k bereits bekannt ist. Mit den vorliegenden Aufzeichnungen wird eine Einführung in elementare algebraische Methoden der Galoiskohomologie gegeben und durch Beispiele erläutert. Dabei orientiert sich die Bereitstellung des algebraischen Rahmens an den entsprechenden Darstellungen in [$SE1$], Chapter X; in [$SE2$], insbesondere Chapter III; sowie in [$H1$]. Die Beispiele, die in diesem Rahmen diskutiert werden, sind endlichdimensionale assoziative zentraleinfache Algebren über einem Körper, nichtausgeartete quadratische Formen über einem Körper

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

mit von 2 verschiedener Charakteristik sowie Twistungen von Körpern. Arithmetische oder arithmetisch-geometrische Aspekte der Galoiskohomologie werden in dem vorliegenden Text kaum besprochen; in dieser Hinsicht verweisen wir auf entsprechende Abschnitte in [AT], [BA], [HB], [KN], [ML], [NK], [NSW], [PT], [PR], [$SE1$], [$SE2$], [SH], [SM], [$T1$], [$T2$]; dabei werden besonders in [KN], [PR] solche arithmetischen Aspekte behandelt, die mit der Theorie der algebraischen Gruppen zusammenhängen. Das Buch [SH] behandelt proendliche Gruppen und ihre Kohomologie bezüglich kommutativer Gruppen, Zusammenhänge zwischen Galoiskohomologie und diophantischen Problemen der Körpertheorie, lokale Klassenkörpertheorie, Dualitätstheorie und schlägt einen Bogen zum Begriff der Grothendiecktopologie und der damit verbundenen Kohomologietheorie.

Diese Aufzeichnungen haben vorläufigen Charakter und erheben keinerlei Anspruch auf Originalität. Sie sollen Grundbegriffe bereitstellen, um das Studium von weiterführender Literatur zur Galoiskohomologie, z.B. von [$SE2$], [$KMRT$], [GMS] und der dort angegebenen Literatur, zu erleichtern.

§ 1. Klassifikationsprobleme in Kategorien über Körpern und die erste Kohomologiemenge

In diesem Abschnitt soll das in der Einleitung angedeutete Klassifikationsproblem genauer formuliert werden. Dabei dienen entsprechende Ausführungen in [$SE1$], Chapter VII, Appendix, und Chapter X; in [$SE2$], Chapter I, §5, Chapter III, §1; sowie in [$H1$] teilweise als Vorlage. Ein wesentlich weiterer Rahmen für die Formulierung und Lösung von allgemeineren Klassifikationsproblemen wurde von A. Grothendieck und J. Giraud entwickelt; vgl.dazu [$SGA1$], Exposé VI; [$G1$], [$G2$] ; und [GI]. Siehe dazu auch die Bemerkungen in [$SE1$], Chapter VII, Appendix, Remarks, 2, und Chapter X, §2, Remark.

Um Paradoxien und widersprüchliche Begriffsbildungen, die sich aus einem naiven Verständnis von Mengen ergeben, zu vermeiden, gibt es verschiedene Vorschläge und Theorien. Für die nachfolgenden Ausführungen, insbesondere für Begriffsbildungen im Zusammenhang mit Kategorien, erweist es sich als günstig, den von A. Grothendieck stammenden Begriff des Universums einzuführen.

Definition Ein *Universum* ist eine Menge $\mathcal{U}$, die folgende Eigenschaften besitzt:

(1) Wenn $A \in \mathcal{U}$, dann ist $A \subset \mathcal{U}$

(2) Wenn $A, B \in \mathcal{U}$, dann ist $\{A, B\} \in \mathcal{U}$

(3) Wenn $A \in \mathcal{U}$, dann ist $\mathfrak{P}(A) \in \mathcal{U}$

(4) Ist $J \in \mathcal{U}$ und existiert zu jedem $j \in J$ genau ein $U_j \in \mathcal{U}$, dann ist die Vereinigung $\cup_{j \in J} U_j$ ebenfalls ein Element von $\mathcal{U}$

vgl. dazu [$SGA4$] , Exposé I, insbesondere Appendice: Univers (par N. Bourbaki); oder [SB], Teil I, 3, S. 15/16.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Aus den in dieser Definition geforderten Eigenschaften von $\mathcal{U}$ ergibt sich, daß bei der Anwendung der üblichen Operationen der Mengenlehre auf Elemente von $\mathcal{U}$ wiederum nur Elemente von $\mathcal{U}$ entstehen. Wir legen deshalb allen Betrachtungen ein fest gewähltes Universum $\mathcal{U}$ zugrunde, in dem jede der vorkommenden Mengen als Element enthalten ist. Eine *Klasse in bezug auf* $\mathcal{U}$ ist eine Teilmenge von $\mathcal{U}$. Nachfolgend auftretende Klassen sind stets Klassen in bezug auf $\mathcal{U}$.

Die nachfolgenden Begriffsbildungen aus der Theorie der Kategorien findet man in vielen einschlägigen Lehrbüchern, z.B. in $[SB]$.

Definition Eine *Kategorie* $\mathfrak{A}$ besteht aus einer Klasse $Ob(\mathfrak{A})$, deren Elemente *Objekte von* $\mathfrak{A}$ genannt werden, und für je zwei Objekte $X, Y \in Ob(\mathfrak{A})$ aus einer Menge $Mor(X, Y)$, deren Elemente *Morphismen von* X *nach* Y genannt werden, so daß für je drei Elemente $X, Y, Z \in Ob(\mathfrak{A})$ eine Abbildung

$$\circ : Mor(Y, Z) \times Mor(X, Y) \to Mor(X, Z)$$

definiert ist, die *Komposition* oder *Verknüpfung* genannt wird, so daß die folgenden Aussagen erfüllt sind:

(i) Die Mengen $Mor(X, Y)$ und $Mor(X', Y')$ sind disjunkt für $X \neq X'$ oder $Y \neq Y'$, und sie sind gleich, wenn $X = X'$ und $Y = Y'$

(ii) Für jedes $X \in Ob(\mathfrak{A})$ existiert ein Element $id_X \in Mor(X, X)$, genannt *Identität auf* X, so daß für alle $Y \in Ob(\mathfrak{A})$ gilt

$id_X \circ f = f$ für alle $f \in Mor(Y, X)$

$g \circ id_X = g$ für alle $g \in Mor(X, Y)$

(iii) Für je drei Elemente $f \in Mor(X, Y)$, $g \in Mor(Y, Z)$, $h \in Mor(Z, W)$ mit $X, Y, Z, W \in Ob(\mathfrak{A})$ gilt

$(h \circ g) \circ f = h \circ (g \circ f)$

Sei $\mathfrak{A}$ eine Kategorie und seien $X, Y \in Ob(\mathfrak{A})$. Morphismen $f \in Mor(X, Y)$ schreiben wir auch wie Abbildungen in der Form $f : X \to Y$. $f \in Mor(X, Y)$ heißt *Isomorphismus*, falls ein $g \in Mor(Y, X)$ existiert, so daß $f \circ g = id_Y$ und $g \circ f = id_X$. Mit $Isom(X, Y)$ bezeichnen wir die Menge aller Isomorphismen in $Mor(X, Y)$. Die Elemente aus $End(X) := Mor(X, X)$ heißen auch *Endomorphismen* von X, und die Isomorphismen in $End(X)$ heißen *Automorphismen* von X. Die Menge aller Automorphismen $Aut(X)$ von X bildet bezüglich der Komposition eine Gruppe.

Definition Seien $\mathfrak{A}$ und $\mathfrak{B}$ Kategorien. Ein *kovarianter* bzw. *kontravarianter Funktor* von $\mathfrak{A}$ nach $\mathfrak{B}$ ist eine Vorschrift $F : \mathfrak{A} \to \mathfrak{B}$, die jedem Objekt $A \in Ob(\mathfrak{A})$ genau ein Objekt $F(A) \in Ob(\mathfrak{B})$ zuordnet, und die jedem Morphismus $f : A \to B$ von $\mathfrak{A}$ genau einen Morphismus $F(f) : F(A) \to F(B)$ bzw. $F(f) : F(B) \to F(A)$ von $\mathfrak{B}$ zuordnet, so daß gilt:

(i) $F(id_A) = id_{F(A)}$ für alle $A \in Ob(\mathfrak{A})$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

(ii) $F(g \circ f) = F(g) \circ F(f)$ bzw. $F(g \circ f) = F(f) \circ F(g)$

für alle Morphismen $f : A \to B$ bzw. $g : B \to C$.

Ein Funktor $F : \mathfrak{A} \to \mathfrak{B}$ heißt *treu* bzw. *voll treu,* falls für je zwei Objekte X, Y von $\mathfrak{A}$ die Abbildung $Mor(X,Y) \to Mor(F(X), F(Y))$, $f \mapsto F(f)$, injektiv bzw. bijektiv ist. Eine Kategorie $\mathfrak{A}$ heißt *konkret,* falls es einen treuen Funktor F von $\mathfrak{A}$ in die Kategorie der Mengen - mit den Mengenabbildungen als Morphismen - gibt. In einer konkreten Kategorie sind mit den Elementen eines Objekts X die Elemente von $F(X)$ gemeint.

Nachfolgend betrachten wir nur konkrete Kategorien.

Definition Zwei Kategorien $\mathfrak{A}$ und $\mathfrak{B}$ heißen *aequivalent*, wenn es Funktoren $F : \mathfrak{A} \to \mathfrak{B}$, $G : \mathfrak{B} \to \mathfrak{A}$ gibt, so daß $G \circ F : \mathfrak{A} \to \mathfrak{A}$ der identische Funktor auf A und $F \circ G : \mathfrak{B} \to \mathfrak{B}$ der identische Funktor auf $\mathfrak{B}$ ist.

Dabei ist die Komposition $G \circ F : \mathfrak{A} \to \mathfrak{C}$ von Funktoren $F : \mathfrak{A} \to \mathfrak{B}$ und $G : \mathfrak{B} \to \mathfrak{C}$ wie folgt definiert: $A \longmapsto G(F(A))$ für jedes Objekt A von $\mathfrak{A}$. $f \mapsto G(F(f))$ für jeden Morphismus f von $\mathfrak{A}$.

Definition Sei $\mathfrak{A}$ eine Kategorie und sei $(A_i)_{i \in I}$ eine Folge von Objekten A_i von $\mathfrak{A}$.. Ein *Produkt* bzw. *Koprodukt* dieser Folge ist ein Tupel $(B, (f_i)_{i \in I})$, wobei B ein Objekt von $\mathfrak{A}$ ist und die f_i eine Folge von Morphismen $f_i : B \to A_i$ bzw. $f_i : A_i \to B$ bilden, so daß gilt: Ist C ein Objekt von $\mathfrak{A}$ und ist $(g_i : C \to A_i)_{i \in I}$ bzw. $(g_i : A_i \to C)_{i \in I}$ eine Folge von Morphismen von $\mathfrak{A}$, dann existiert genau ein Morphismus $h : C \to B$ bzw. $h : B \to C$, so daß für alle $i \in I$ gilt: $f_i \circ h = g_i$ bzw. $h \circ f_i = g_i$. Das Objekt B von $\mathfrak{A}$ wird auch mit

$$\prod_{i \in I} A_i \quad \text{bzw.} \quad \coprod_{i \in I} A_i$$

bezeichnet, und die Morphismen f_i werden *Projektionen* bzw. *Inklusionen* genannt.

Produkte und Koprodukte existieren nicht in jeder Kategorie.

Definition (Vgl. auch [$H1$], 2.1.2) Sei G eine Gruppe und sei $\mathfrak{A}$ eine Kategorie. Sei A ein Objekt von $\mathfrak{A}$. Eine *Anwendung von G von links auf A* ist eine Abbildung $G \times A \to A$, $(s, a) \mapsto s(a) = a^s$, so daß gilt:

(1) $e_G(a) = a$ für alle $a \in A$, wobei e_G das neutrale Element von G bezeichnet

(2) $a^{st} = (a^t)^s$ für alle $a \in A$ und alle $s, t \in G$.

Eine *Operation* von *G von links auf A* ist eine Anwendung von G von links auf A, so daß jedes $s \in G$ zu einem Endomorphismus von A wird, d.h. die Abbildung $A \to A$, $a \mapsto a^s$, ist ein Endomorphismus von A. Entsprechend definiert man *Anwendungen* und *Operationen von rechts.*

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Die folgende Bemerkung ist leicht zu beweisen

(1.1) **Bemerkung** Aequivalent sind
(a) G operiert auf A
(b) Es existiert ein Homomorphismus von Gruppen $G \to Aut(A)$

Ein Objekt A einer Kategorie $\mathfrak{A}$ zusammen mit einer Anwendung der Gruppe G auf A heißt auch *G-Objekt* von A; und eine Abbildung $f : A \to B$ von G-Objekten heißt *G-Abbildung* oder *G-equivariante* oder *G-verträgliche* Abbildung, wenn $f(s(a)) = s(f(a))$ für alle $a \in A$ und alle $s \in G$ gilt. Die G-Objekte einer Kategorie zusammen mit den G-Abbildungen als Morphismen bilden eine Kategorie. Ähnliches gilt für die Objekte einer Kategorie, auf denen eine Gruppe operiert. Ist insbesondere $\mathfrak{A}$ die Kategorie, deren Objekte Gruppen und deren Morphismen Gruppenhomomorphismen sind, und operiert die Gruppe G auf $A \in Ob(\mathfrak{A})$, dann heißt A auch *G-Gruppe*. Ist A zusätzlich abelsch, dann heißt A auch *G-Modul*. Sind A und B G-Gruppen und ist $\psi : A \to B$ ein Gruppenhomomorphismus, dann heißt ψ ein *G-Homomorphismus*, falls ψ *G-verträglich* ist, d.h. falls $\psi(s(a)) = s(\psi(a))$ für alle $a \in A$, $s \in G$ gilt. Die G-Gruppen zusammen mit den G-Homomorphismen als Morphismen bilden eine Kategorie. Ist ψ ein G-Isomorphismus, d.h. ein bijektiver G-Homomorphismus, so auch ψ^{-1}. Eine *exakte G-Sequenz* ist eine exakte Sequenz von G-Gruppen, deren Homomorphismen G-verträglich sind. Die Bezeichnung "G-verträglich" wird sinngemäß auch für Morphismen ψ beliebiger Kategorien gebraucht.

Eine *punktierte Menge* ist ein Paar bestehend aus einer Menge und einem Element dieser Menge, das auch *ausgezeichnetes Element* genannt wird. Ein *Homomorphismus punktierter Mengen* ist eine Mengenabbildung, die das ausgezeichnete Element auf das ausgezeichnete Element abbildet. Der *Kern* eines Homomorphismus von punktierten Mengen ist das Urbild des ausgezeichneten Elementes. Damit ist auch der Begriff der *exakten Sequenz* punktierter Mengen definiert.

Definition (Vgl. auch [$H1$], 2.3.1) Sei $\mathfrak{C}$ eine Kategorie. Eine durch $\mathfrak{C}$ *indizierte Kategorie* ist eine Kategorie von Kategorien $\mathfrak{F}$ zusammen mit einem kovarianten Funktor von $\mathfrak{C}$ in $\mathfrak{F}$; ausführlicher: Für jedes Objekt $K \in Ob(\mathfrak{C})$ ist genau eine Kategorie $\mathfrak{F}_K \in Ob(\mathfrak{F})$ gegeben, und für jeden Morphismus $r \in Mor(K, L)$ in $\mathfrak{C}$ ist genau ein kovarianter Funktor $r_{L/K} = r_* : \mathfrak{F}_K \to \mathfrak{F}_L$ definiert, so daß $(id_K)_* = id_{\mathfrak{F}_K}$ für jedes Objekt $K \in Ob(\mathfrak{C})$ und so daß für je zwei Morphismen $r \in Mor(K, L)$, $r' \in Mor(L, M)$ in $\mathfrak{C}$ die Gleichung $(r' \circ r)_* = r'_* \circ r_*$ erfüllt ist.

Für das Bild eines Objekts X aus $\mathfrak{F}_K$ unter $r_{L/K}$ bzw. für das Bild $r_{L/K}(f)$ eines Morphismus f von $\mathfrak{F}_K$ unter $r_{L/K}$ wird auch die suggestive Bezeichnung

$$X \times_K L = X_L \text{ bzw. } f_L = f \times_K L$$

verwendet.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Definition (Vgl. auch [$H1$], 2.1.2) Sei k ein Körper. Eine *Kategorie von Körpererweiterungen von* k ist eine Kategorie $\mathfrak{G}(k)$, deren Objekte Körpererweiterungen von k und deren Morphismen Inklusionen von Körpererweiterungen von k sind, d.h. für $K, L \in Ob(\mathfrak{G}(k))$ ist $Mor(K, L) = \{K \subset L\}$, falls K ein Teilkörper von L ist, und $Mor(K, L) = \emptyset$ andernfalls. Eine k-*Kategorie* oder eine *Kategorie über* k ist eine durch eine Kategorie von Körpererweiterungen $\mathfrak{G}(k)$ indizierte Kategorie $\mathfrak{F}$, so daß für je zwei Objekte $K, L \in Ob(\mathfrak{G}(k))$ mit der Eigenschaft, daß L/K eine endliche Galoiserweiterung ist, und für jedes Objekt $X \in Ob(\mathfrak{F}_K)$ eine Anwendung der Galoisgruppe $G(L/K)$ von L/K auf $X_L = r_{L/K}(X) \in Ob(\mathfrak{F}_L)$ definiert ist, so daß für je zwei Objekte $X, Y \in Ob(\mathfrak{F}_K)$ gilt: Wenn $s \in G(L/K)$ und $f \in Isom(X_L, Y_L)$, dann ist $f^s := s \circ f \circ s^{-1} \in Isom(X_L, Y_L)$.

Die Aussagen in der nachfolgenden Bemerkung bestätigt man durch direktes Nachrechnen.

(1.2) **Bemerkung** (Vgl. auch [$H1$], Proposition 2.3-2) Sei $\mathfrak{F}$ eine k-Kategorie, die durch die Kategorie von Körpererweiterungen $\mathfrak{G}(k)$ von k indiziert ist. Dann gilt

(i) $e_{G(L/K)}(f) = f$
(ii) $f^{st} = (f^t)^s$
(iii) $(g \circ f)^s = g^s \circ f^s$
(iv) $id^s_{X_L} = id_{X_L}$
(v) $(f^{-1})^s = (f^s)^{-1}$

jeweils für alle $K, L \in Ob(\mathfrak{G}(k))$ mit der Eigenschaft, daß L/K eine endliche Galoiserweiterung ist, alle Objekte $X, Y, Z \in Ob(\mathfrak{F}_K)$ und alle $f \in Isom(X_L, Y_L)$, $g \in Isom(Y_L, Z_L)$, und alle $s, t \in G(L/K)$.

Insbesondere operiert $G(L/K)$ auf jeder Automorphismengruppe $Aut(X_L)$.

Ist $\mathfrak{F}$ eine durch $\mathfrak{G}(k)$ indizierte k-Kategorie und sind K, L Objekte von $\mathfrak{G}(k)$, so daß L/K Körpererweiterung ist, so wird für jedes Objekt X von $\mathfrak{F}_K$ das Bild $X_L = r_{L/K}(X)$ von X unter $r_{L/K}$ als *Skalarereiterung von X mit L* bezeichnet; und ist $f \in Mor(X, Y)$ ein Morphismus in $\mathfrak{F}_K$, so wird der Morphismus $f_L := r_{L/K}(f) \in Mor(X_L, Y_L)$ auch als *L-Fortsetzung* von f bezeichnet.

Definition (Vgl. auch [$H1$], 2.3.1) Eine durch $\mathfrak{G}(k)$ indizierte k-Kategorie $\mathfrak{F}$ heißt *fortsetzend,* falls für je zwei Objekte K, L von $\mathfrak{G}(k)$ mit der Eigenschaft, daß L/K eine endliche Galoiserweiterung ist, und für je zwei Objekte X, Y von $\mathfrak{F}_K$ und jeden Morphismus $f \in Mor(X_L, Y_L)$ gilt:

$f \in r_{L/K}(Isom(X, Y))$ genau dann, wenn $f \in Isom(X_L, Y_L)^{G(L/K)}$.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Eine *Galoiskategorie über* k ist eine fortsetzende k-Kategorie $\mathfrak{F}$; und wenn $\mathfrak{F}$ durch die Kategorie von Körpererweiterungen $\mathfrak{G}(k)$ indiziert ist, dann sagt man auch: $\mathfrak{F}$ ist eine *Galoiskategorie über* $\mathfrak{G}(k)$.

(1.3) **Beispiel** Für jede Körpererweiterung K/k sei $\mathfrak{F}_K$ die Kategorie der endlichdimensionalen K-Vektorräume, und für jede Körpererweiterung L/K sei $r_{L/K} : \mathfrak{F}_K \to \mathfrak{F}_L$ der Funktor, der durch Skalarerweiterung von K zu L gegeben ist, genauer: Jedem endlichdimensionalen K-Vektorraum V wird der endlichdimensionale L-Vektorraum $V_L := V \otimes_K L$ und jedem Homomorphismus $f : V \to W$ von endlichdimensionalen K-Vektorräumen wird der Homomorphismus von L-Vektorräumen $f_L : V_L \to W_L$, $f_L(v \otimes \lambda) := f(v) \otimes \lambda$ zugeordnet. Ist L/K eine endliche Galoiserweiterung und ist V ein endlichdimensionaler K-Vektorraum, dann wird durch die Zuordnung $G(L/K) \times V_L \to V_L$, $(s, v \otimes \lambda) \mapsto v \otimes s(\lambda)$, $s \in G(L/K)$, $v \in V$, $\lambda \in L$, eine Anwendung der Galoisgruppe $G(L/K)$ auf V_L definiert. Die entsprechenden Abbildungen $\underline{s} : V_L \to V_L$, $s \in G(L/K)$ sind bijektive s-semilineare Abbildungen. Außerdem ist $g^s = s \circ g \circ s^{-1} \in Isom(V_L, W_L)$ für alle $g \in Isom(V_L, W_L)$ und für alle $s \in G(L/K)$. Sei $f \in Isom(V, W)$. Dann ist $f_L^s = f_L$ für alle $s \in G(L/K)$; denn für alle $v \in V$ und alle $\lambda \in G(L/K)$ gilt $f_L^s(v \otimes \lambda) = s(f(v) \otimes s^{-1}(\lambda)) = f(v) \otimes \lambda = f(v \otimes \lambda)$. Sei umgekehrt $g \in Isom(V_L, W_L)^{G(L/K)}$. Sei (v_i) eine K-Basis von V. Dann ist $(v_i \otimes 1_L)$ eine L-Basis von V_L; denn eine nichttriviale lineare Relation zwischen den $v_i \otimes 1_L$ hätte eine nichttriviale lineare Relation zwischen den v_i zur Folge, wie man unter Beachtung der Separabilität von L/K - nach R. Dedekind - durch Spurbildung erkennt. Sei weiterhin (w_j) eine K-Basis von W. Es ist dann $g^s(v_i \otimes 1_L) = s(g(v_i \otimes 1_L) = s(\Sigma_j a_{ij}(w_j \otimes 1_L))$ mit $a_{ij} \in L$, so daß die Matrix (a_{ij}) invertierbar ist; und dieser Ausdruck ist gleich $\Sigma_j s(a_{ij})(w_j \otimes 1_L) = \Sigma_j a_{ij}(w_j \otimes 1_L) = g(v_i \otimes 1_L)$. Somit gilt $s(a_{ij}) = a_{ij}$ für alle $s \in G(L/K)$, also $a_{ij} \in K$. Definiert man $f(v_i) := \Sigma_j a_{ij} w_j$, dann ist $f \in Isom(V, W)$, und es gilt $g = f_L$. Man erhält also eine Galoiskategorie $\mathfrak{F} = \mathfrak{V}$ über k, die wir auch die *Galoiskategorie der Vektorräume über* k nennen.

Sei nun $\mathfrak{F}$ eine Galoiskategorie über $\mathfrak{G}(k)$. Seien $L, K \in Ob(\mathfrak{G}(k))$, so daß L/K eine Körpererweiterung ist. Ein K-*Objekt* von $\mathfrak{F}$ ist ein Objekt von $\mathfrak{F}_K$. Sei X ein festes K-Objekt. Ein K-Objekt Y heißt L/K-Twistung von X oder L/K-Form von X, falls X_L und Y_L isomorph sind, d.h. falls $Isom(X_L, Y_L) \neq \emptyset$. Sei

$$E(L/K, X) = E_{\mathfrak{F}}(L/K, X)$$

die Menge aller K-Isomorphieklassen von L/K-Twistungen von X; vgl. dazu auch $[SE1]$, Chapter X, sowie $[H1]$, 2.3.2. Diese Menge ist wohldefiniert, d.h. jedes Objekt Y' aus einer Isomorphieklasse (Y) von L/K-Twistungen von X ist wieder eine L/K-Twistung von X; denn für $f \in Isom(Y, Y')$ ist $r_{L/K}(f) : Y_L \to Y'_L$ ein Isomorphismus:

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$r_{L/K}(f) \circ r_{L/K}(f^{-1}) = r_{L/K}(f \circ f^{-1}) = id_{Y'_L}$
$r_{L/K}(f^{-1}) \circ r_{L/K}(f) = r_{L/K}(f^{-1} \circ f) = id_{Y_L}$

Eine wichtige Aufgabe ist die Bestimmung der Mengen $E_{\mathfrak{F}}(L/K, X)$ für gewisse Galoiskategorien $\mathfrak{F}$. Dafür kann man kohomologische Methoden einsetzen, die wir nun beschreiben; dabei folgen wir den entsprechenden Ausführungen in [SE1], Chapter VII, Appendix, und Chapter X, sowie [SE2], Chapter I, §5 und Chapter III.

Sei G eine Gruppe, die von links auf einer nichtleeren Menge X operiert. Sei

$$H^0(G, X) := X^G := \{x \in X : s(x) = x \text{ für alle } s \in G\}.$$

Ist A eine - nicht notwendigerweise kommutative - Gruppe, auf der G von links durch Automorphismen von A operiert, dann ist $H^0(G, A)$ eine Untergruppe von A, die sogenannte *0-te Komologiegruppe von G mit Koeffizienten in A*.

Ein 1-*Kozykel von G in A* ist eine Abbildung $\alpha : G \to A$, $s \mapsto \alpha(s) = a_s$, so daß $a_{st} = a_s s(a_t)$ für alle $s, t \in G$. Sei $Z^1(G, A)$ die Menge aller 1-Kozykeln $G \to A$. Zwei 1-Kozykeln $\alpha, \beta \in Z^1(G, A)$, $\alpha(s) = a_s$, $\beta(s) = b_s$, heißen *kohomolog* oder *aequivalent*, falls ein $a \in A$ existiert, so daß $b_s = a^{-1} a_s s(a)$ für alle $s \in G$. Es handelt sich hierbei um eine Aequivalenzrelation. Die Menge der entsprechenden Aequivalenzklassen (α), $\alpha \in Z^1(G, A)$, wird mit $H^1(G, A)$ bezeichnet. $H^1(G, A)$ besitzt ein ausgezeichnetes Element, nämlich die Klasse des 1-Kozykels $\mathtt{1} : s \mapsto a_s = 1$ für alle $s \in G$. $H^1(G, A)$ heißt die *1-te Kohomologiemenge von G mit Werten in A*.

$H^0(G, -)$ und $H^1(G, -)$ sind Funktoren in A. Insbesondere gilt: Ist $f : A \to B$ ein G-Homomorphismus, dann erhält man Abbildungen

$$f_0 : H^0(G, A) \to H^0(G, B), \quad f_1 : H^1(G, A) \to H^1(G, B)$$

wie folgt: f_0 ist die Restriktion von f auf A^G; für jeden 1-Kozykel $\alpha : G \to A$ ist $f_1((\alpha))$ definiert als die Klasse des 1-Kozykels $G \xrightarrow{\alpha} A \xrightarrow{f} B$.

f_0 ist ein Homomorphismus von Gruppen; f_1 ist eine Abbildung von punktierten Mengen, es gilt also $f_1((\mathtt{1})) = (\mathtt{1})$.

Uns interessiert insbesondere der Fall, in dem der G-Homomorphismus $f : A \to B$ injektiv ist. Vermöge dieser Einbettung betrachten wir A als Untergruppe von B, die unter der Operation von G in sich überführt wird. Die Menge $B \setminus A$ aller Linksnebenklassen bA, $b \in B$, ist bezüglich der Abbildung $G \times (B \setminus A) \to B \setminus A$, $(s, bA) \mapsto s(b)A$, eine G-Menge. $H^0(G, B \setminus A)$ ist dann die Kohomologiemenge der unter allen Elementen von G invarianten Elemente aus $B \setminus A$ mit der Nebenklasse A als ausgezeichnetem Element, und die Abbildung $H^0(G, B) \to H^0(G, B \setminus A)$, $b \mapsto bA$, ist ein Homomorphismus von punktierten Mengen. Man definiert eine Korandabbildung

$$\delta : H^0(G, B \setminus A) \to H^1(G, A)$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

wie folgt: Für $c \in (B \setminus A)^G$ sei $b \in B$ ein Repräsentant. Setze $a_s := b^{-1}b^s$. Die so definierte Abbildung $\alpha : G \to A$, $\alpha(s) := a_s$, ist ein 1-Kozykel. Wir setzen $\delta(c) := (\alpha) \in H^1(G, A)$. Nach Konstruktion wird (α) unter der durch $f : A \to B$ induzierten Abbildung $H^1(G, A) \to H^1(G, B)$ trivial. Umgekehrt ist jedes Element aus $H^1(G, A)$, das unter dieser Abbildung trivial wird, von der Form $\delta(c)$ für ein $c \in (B \setminus A)^G$. Es folgt, vgl. [$SE2$], Chapter I, §5, Proposition 36,

(1.4) **Satz** *Die durch den G-Homomorphismus $f : A \to B$ und die soeben definierte Korandabbildung $\delta : H^0(G, B \setminus A) \to H^1(G, A)$ induzierte Sequenz von punktierten Kohomologiemengen*

$$1 \to H^0(G, A) \to H^0(G, B) \to H^0(G, B \setminus A) \xrightarrow{\delta} H^1(G, A) \xrightarrow{f_1} H^1(G, B)$$

ist exakt.

Wenn das Bild des G-Homomorphismus $f : A \to B$ eine normale Untergruppe von B ist, dann ist $B \setminus A$ eine G-Gruppe, die wir mit C bezeichnen, und der G-Homomorphismus $g : B \to C$, $b \mapsto bA$, induziert eine Abbildung von punktierten Kohomologiemengen $H^1(G, B) \to H^1(G, C)$. Aus der Konstruktion folgt $g_1 \circ f_1 = id$. Außerdem ist ein 1-Kozykel, der nach Komposition mit $g : B \to C$ kohomolog zu dem trivialen 1-Kozykel wird, in B kohomolog zu einem 1-Kozykel in $f(A)$. Aus diesen Bemerkungen ergibt sich mit dem vorstehenden Satz die folgende Aussage, vgl. [$SE1$], Chapter VII, Appendix, Proposition 1.

(1.5) **Satz** *Angenommen das Bild des G-Homomorphismus von G-Gruppen $f : A \to B$ ist eine normale Untergruppe von B. Dann ist die Faktorgruppe $C := B/f(A)$ eine G-Gruppe, und die G-Homomorphismen $f : A \to B$ und $g : B \to C$ induzieren die folgende exakte Sequenz von Kohomologiemengen*

$$1 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G, A) \xrightarrow{f_1} H^1(G, B) \xrightarrow{g_1} H^1(G, C)$$

Wir wollen nun einen Zusammenhang zwischen Galoiskategorien und der 1-ten Kohomologiemenge herstellen. Sei dazu k ein Körper, sei $\mathfrak{F}$ eine Galoiskategorie über $\mathfrak{G}(k)$, seien $K, L \in Ob(\mathfrak{G}(k))$, so daß L/K eine endliche Galoiserweiterung ist, und sei X ein K-Objekt von $\mathfrak{F}$. Sei $E(L/K, X) = E_{\mathfrak{F}}(L/K, X)$ die Menge aller K-Isomorphieklassen (Y) von L/K-Twistungen oder L/K-Formen Y von X. Man definiert eine Abbildung

(1.6) $\quad \theta : E_{\mathfrak{F}}(L/K, X) \to H^1(G(L/K), Aut(X_L))$

wie folgt, vgl. [$SE1$], Chapter X, §2, sowie [$H1$], Satz 2.3-3: Für $(Y) \in E_{\mathfrak{F}}(L/K, X)$ sei $f : X_L \to Y_L$ ein L-Isomorphismus. Dann ist $f^{-1} \circ f^s \in Aut(X_L)$ für alle $s \in G(L/K)$ ein L-Automorphismus, und die Zuordnung $p : G(L/K) \to Aut(X_L)$, $s \mapsto p_s := f^{-1} \circ f^s$, ist ein 1-Kozykel:

$$p_s p_t^s = (f^{-1} \circ f^s) \circ (f^{-1} \circ f^t)^s = f^{-1} \circ f^s \circ (f^s)^{-1} \circ f^{st} = f^{-1} \circ f^{st} = p_{st}.$$

Ist $f' \in Isom(X_L, Y_L)$ ein weiterer Isomorphismus, dann ist $g := f^{-1} \circ f' \in Aut(X_L)$, und es gilt

$$p'_s = f'^{-1} \circ f'^s = g^{-1} \circ f^{-1} \circ f^s \circ g^s = g^{-1} \circ p_s \circ g^s,$$

d.h. die 1-Kozykeln p und p' sind aequivalent.

Sei Y' ein zu Y K-isomorphes K-Objekt und sei $g \in Isom(Y, Y')$ ein Isomorphismus. Dann ist $g_L := r_{L/K}(g) \in Isom(Y_L, Y'_L)$ ein Isomorphismus, der invariant unter $G(L/K)$ ist; denn die Kategorie $\mathfrak{F}$ ist nach Voraussetzung fortsetzend. Es gilt also $g_L^{-1} \circ g_L^s = id_{Y_L}$ für alle $s \in G(L/K)$, und $f' := g_L \circ f \in Isom(X_L, Y'_L)$. Somit ist

$$p''_s := f'^{-1} \circ f'^s = f^{-1} \circ g_L^{-1} \circ g_L^s \circ f^s = f^{-1} \circ f^s = p_s.$$

Die Abbildung θ ist also wohldefiniert.

Wir zeigen, daß θ injektiv ist. Seien dazu $Y, Y' \in E_{\mathfrak{F}}(L/K, X)$ L/K-Twistungen von X, sei $f \in Isom(X_L, Y_L)$ und sei $f' \in Isom(X_L, Y'_L)$. Angenommen es gilt

$$\theta((Y)) = \theta((Y')), \text{ d.h. } (p : s \mapsto p_s = f^{-1} \circ f^s) = (p' : s \mapsto p'_s = f'^{-1} \circ f'^s).$$

Dann existiert ein $g \in Aut(X_L)$, so daß $p'_s = g^{-1} \circ p_s \circ g^s$ für alle $s \in G(L/K)$, oder, dazu aequivalent, $f' \circ g^{-1} \circ f^{-1} = (f'' \circ g^{-1} \circ f^{-1})^s$ für alle $s \in G(L/K)$. Für $h := f' \circ g^{-1} \circ f^{-1} \in Isom(Y_L, Y'_L)$ gilt also $h^s = h$ für alle $s \in G(L/K)$. Da die Kategorie $\mathfrak{F}$ fortsetzend ist, existiert ein $h' \in Isom(Y, Y')$ mit $r_{L/K}(h') = h$. Somit ist $(Y) = (Y')$.

Wir fassen zusammen

(1.7) **Satz** *Die unter (1.6) definierte Abbildung θ ist injektiv.*

Der nachfolgende Satz, der in der Sprache der semilinearen Abbildungen von A. Speiser, vgl. [SP], Satz 1, bewiesen wurde, ist für den Aufbau der Galoiskohomologie von großer Bedeutung.

(1.8) **Satz** *Für alle natürlichen Zahlen n und alle endlichen Galoiserweiterungen L/K gilt $H^1(G(L/K), GL(n, L)) = 1$.*

Im Beweis folgen wir der Darstellung in [$SE1$], chap. X, § 1. Wesentliches Hilfsmittel ist dabei die von R. Dedekind entdeckte lineare Unabhängigkeit der

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Charaktere, die von E. Artin für den Aufbau der Galoistheorie verwendet wurde, vgl. [A]; insbesondere II, Abschnitt F.

Definition Sei G eine multiplikativ geschriebene Gruppe und sei K ein Körper. Ein *Charakter von G in K* ist ein Homomorphismus $\sigma : G \to K^*$.

Die Menge aller Abbildungen von G nach K bildet bezüglich der punktweise erklärten Addition und Skalarmultiplikation einen K-Vektorraum, der die Charaktere von G in K enthält.

(1.9) **Satz** (Lineare Unabhängigkeit der Charaktere) *Für alle natürlichen Zahlen n sind je n paarweise verschiedene Charaktere $\sigma_1, ..., \sigma_n$ von G in K linear unabhängig im K-Vektorraum aller Abbildungen von G nach K.*

Beweis (genau wie in [A], II, Abschnitt F, S. 28 ff): Zu zeigen ist: Sind für Elemente $a_1, ..., a_n \in K$ die Gleichungen

$$a_1\sigma_1(x) + a_2\sigma_2(x) + ... + a_n\sigma_n(x) = 0$$

für alle $x \in G$ erfüllt, dann gilt $a_1 = a_2 = ... = a_n = 0$. Das beweist man durch Induktion über n: Für $n = 1$ folgt aus $a_1\sigma_1(x) = 0$ sofort $a_1 = 0$, weil $\sigma_1(x) \neq 0$. Sei nun $n > 1$ und sei die Behauptung für weniger als n Charaktere richtig. Eine hypothetische Relation der Form

$$(*) \quad a_1\sigma_1(x) + a_2\sigma_2(x) + ... + a_n\sigma_n(x) = 0$$

wird auf zweierlei Art umgeformt:

(1) x wird ersetzt durch yx, wobei $y \in G$
(2) (*) wird mit $\sigma_n(y)$ multipliziert

Die beiden so erhaltenen Relationen sind

$$a_1\sigma_1(y)\sigma_1(x) + a_2\sigma_2(y)\sigma_2(x) + ... + a_n\sigma_n(y)\sigma_n(x) = 0$$
$$a_1\sigma_n(y)\sigma_1(x) + a_2\sigma_n(y)\sigma_2(x) + ... + a_n\sigma_n(y)\sigma_n(x) = 0$$

Substraktion der zweiten von der ersten Gleichung ergibt

$$a_1(\sigma_1(y) - \sigma_n(y))\sigma_1(x) + ... + a_{n-1}(\sigma_{n-1}(y) - \sigma_n(y))\sigma_{n-1}(x) = 0$$

Aus der Induktionsannahme folgt insbesondere

$$a_1(\sigma_1(y) - \sigma_n(y)) = 0.$$

Wegen $n > 1$ sind die Charaktere σ_1 und σ_n verschieden. Also existiert ein $y \in G$ mit der Eigenschaft $\sigma_1(y) \neq \sigma_n(y)$. Bei dieser Wahl von y ist

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$a_1 = 0$. Trägt man dies in die ursprüngliche Relation (*) ein, so folgt aus der Induktionsannahme auch $a_2 = ... = a_n = 0$.

Wir wenden diesen Satz auf den Fall an, in dem G die multiplikative Gruppe eines Körpers E ist, und die Charaktere aus Monomorphismen von E in einen Körper E' hervorgehen, und erhalten

(1.10) **Folgerung** *Sind E und E' zwei Körper und sind $\sigma_1, \sigma_2, ..., \sigma_n$ paarweise verschiedene Isomorphismen von E in E', dann sind $\sigma_1, \sigma_2, ..., \sigma_n$ linear unabhängig im E'-Vektorraum aller Abbildungen von E^* nach E'.*

Wir wenden uns nun dem Beweis von (1.8) zu und führen ihn zunächst für den Fall $n = 1$, also für die Aussage

$$H^1(G, L^*) = 1,$$

durch, vgl. $[SE1]$, Chapter X, §1. Sei dazu $\alpha : G \to L^*, \alpha(s) = a_s$, ein 1-Kozykel. Für $c \in L^*$ sei

$$b_c := b := \sum_{s \in G} a_s s(c).$$

Wegen der linearen Unabhängigkeit der $s \in G$ kann man $c \in L^*$ so wählen, daß $b = b_c \neq 0$. Außerdem gilt für alle $s \in G$

$$s(b) = \sum_{t \in G} s(a_t) st(c) = \sum_{t \in G} a_s^{-1} a_{st} st(c) = a_s^{-1} \cdot b,$$

d.h. α ist ein Korand.

Beweis von (1.8), vgl. $[SE1]$, Chapter X, §1: Sei

$$\alpha : G \to GL(n, L),\ \alpha(s) = a_s,$$

ein 1-Kozykel. Für $x \in L^n$ setze

$$b(x) := \sum_{s \in G} a_s(s(x)).$$

Behauptung: Die Vektoren $b(x)$, $x \in L$, erzeugen L^n als L-Vektorraum.
Beweis: Es reicht zu zeigen, daß jede L-Linearform $u : L^n \to L$, die auf allen Vektoren $b(x)$, $x \in L^n$, Null ist, trivial ist. Sei also $u(b(x)) = 0$ für alle $x \in L^n$. Dann gilt für jedes $h \in L$

$$0 = u(b(h(x))) = \sum_{s \in G} u(a_s(s(h)s(x))) = \sum_{s \in G} s(h)u(a_s s(x)).$$

Wegen der linearen Unabhängigkeit der Abbildungen $s : L^* \to L$ folgt

$$u(a_s s(x)) = 0 \text{ für alle } s \in G.$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Da die Matrizen a_s, $s \in G$, alle invertierbar sind, ist jedes Element von L^n von der Form $a_s s(x)$ und daher $u = 0$.

Seien nun $x_1, ..., x_n \in L^n$ so gewählt, daß die Vektoren

$$y_1 := b(x_1), ..., y_n := b(x_n)$$

linear unabhängig über L sind. Sei $c \in GL(n, L)$ die Matrix, die - als lineare Abbildung - für alle $i = 1, ..., n$ den kanonischen Basisvektor e_i von L^n, bei dem an der i-ten Stelle die 1 und sonst stets die 0 steht, auf den Vektor x_i abbildet. Dann gilt für

$$b_c := b := \sum_{s \in G} a_s s(c)$$

die Gleichung

$$b(e_i) = y_i \text{ für alle } i = 1, ..., n.$$

Also ist b invertierbar. Es folgt

$$s(b) = s(\sum_{t \in G} a_t t(c)) = \sum_{t \in G} s(a_t) st(c) = \sum_{t \in G} a_s^{-1} a_{st} st(c) = a_s^{-1} \cdot b.$$

Der 1-Kozykel $\alpha : s \mapsto a_s$ ist somit ein Korand. Damit ist der Beweis von (1.8) beendet.

(1.11) **Folgerung** (vgl. [$SE1$], Chapter X, §1) *Für alle natürlichen Zahlen n und alle endlichen Galoiserweiterungen L/K mit Galoisgruppe G gilt*

$$H^1(G, SL(n, L)) = 1$$

Beweis: Die exakte Sequenz von G-Gruppen

$$1 \to SL(n, L) \to GL(n, L) \xrightarrow{\det} L^* \to 1$$

ergibt nach (1.4) die exakte Sequenz von punktierten Kohomologiemengen

$$H^0(G, GL(n, L)) \to H^0(G, L^*) \to H^1(G, SL(n, L)) \to$$

$$\to H^1(G, GL(n, L)) = 1,$$

also die exakte Sequenz

$$GL(n, K) \xrightarrow{\det} K^* \to H^1(G, SL(n, L)) \to 1.$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Da der Determinantenhomomorphismus det : $GL(n, K) \to K^*$ surjektiv ist, folgt die Behauptung.

(1.12) **Bemerkung** Wie in (1.3) erläutert wurde, bilden die endlichdimensionalen Vektorräume über Körpererweiterungen von k und die Homomorphismen zwischen ihnen eine Galoiskategorie $\mathfrak{V}$ über k. Die Automorphismengruppe eines n-dimensionalen K-Vektorraums ist isomorph zur allgemeinen linearen Gruppe $GL(n, K)$. Ist L/K eine endliche Galoiserweiterung, so operiert die Galoisgruppe $G = G(L/K)$ auf $GL(n, L)$ durch $s(A) = (a_{ij}^s)$ für alle $A = (a_{ij}) \in GL(n, L)$ und alle $s \in G$. Aus Satz (1.8) ergibt sich in Verbindung mit (1.7) die wohlbekannte Tatsache, daß die Mengen $E_{\mathfrak{V}}(L/K, V)$ stets aus nur einem Element bestehen.

Wir beschreiben nun eine Verallgemeinerung von Satz (1.8), die in $[SR]$, Appendix, in $[KL]$ und in $[KN]$,Chapter I, 1.7, Beispiel 1, bewiesen wird. Sei dazu L/K eine endliche Galoiserweiterung mit Galoisgruppe $G = G(L/K)$ und sei U eine endlichdimensionale assoziative L-Algebra mit Einselement 1_U. Vermöge der Abbildung $L \to U$, $a \mapsto a1_U$, betrachten wir L als Teilkörper des Zentrums von U. Wir nehmen an, daß G durch Automorphismen auf der Algebra U so operiert, daß die Einschränkung dieser Operation auf L die Galoisoperation von G auf L ist. Die Operation von G auf U induziert eine Operation auf der Einheitengruppe U^* von U.

(1.13) **Satz** *Mit den obigen Bezeichnungen gilt* $H^1(G, U^*) = 1$

Aufgaben und Beispiele

(1) Nimmt man als Objekte die Mengen, die einem vorgegebenem Universum entstammen, und als Morphismen die Relationen - mit der üblichen Verknüpfung von Relationen als Komposition dieser Morphismen - , dann erhält man eine Kategorie. (Vgl. z.B. $[SB]$, Teil I, 1.2.7)

(2) Wiederholen Sie die Hauptresultate über Operationen von Gruppen auf Mengen. Formulieren Sie für die Operation einer endlichen Gruppen auf einer endlichen Menge das Lemma von Burnside. (Vgl. Bücher über Gruppentheorie)

(3) Sei G eine endliche Gruppe und sei $\mathbb{Z}[G]$ die Gruppenalgebra von G über $\mathbb{Z}$. Zeigen Sie, daß die Kategorie der G-Moduln aequivalent zur Kategorie der $\mathbb{Z}[G]$-Moduln ist. (Vgl. Bücher über Algebra, insbesondere über Kohomologie von Gruppen)

(4) Sei K/k eine endliche Galoiserweiterung mit zyklischer Galoisgruppe G, die durch $s \in G$ erzeugt werde. Zeigen Sie: Gilt für $\alpha \in K$ die Gleichung $N_{K/k}(\alpha) = 1$, dann existiert ein $\beta \in K$ mit $\alpha = \beta/s(\beta)$. (Vgl. z.B. $[A]$, II, Abschnitt L)

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

§ 2. Vektorielle Galoiskategorien

In diesem Abschnitt sollen Beispiele von Galoiskategorien angegeben werden, für die die in (1.6) definierte Abbildung nicht nur injektiv sondern auch surjektiv ist, so daß also in solchen Kategorien das in § 1 formulierte Klassifikationsproblem auf die Berechnung der zugehörigen 1-Kohomologiemengen zurückgeführt werden kann; solche Galoiskategorien nennen wir *kohomologisch*. Wie man aus [$SE1$], X, § 2, ersieht, erhält man Beispiele von kohomologischen Galoiskategorien mit Hilfe von tensoriellen Strukturen; diese Konstruktionen werden zunächst erläutert.

Sei k ein Körper.

Definition (Vgl. [$SE1$], Chapter X, §2) Ein *tensorielles k-Objekt vom Typ* (p,q) für $p,q \in \{0,1,2,...\}$ ist ein Paar (V,x) bestehend aus einem endlichdimensionalen k-Vektorraum V und einem Tensor x vom Typ (p,q) auf V, d.h. $x \in \otimes^p V \otimes \otimes^q V^*$, wobei $\otimes^p V$ das p-fache Tensorprodukt von V mit sich selbst bezeichnet (mit der Vereinbarung $\otimes^0 V = k$) und $V^* = Hom(V,k)$ der Dualraum von V ist.

Mit Hilfe der tensoriellen Objekte vom Typ (p,q) läßt sich eine k-Kategorie $\mathfrak{T} = \mathfrak{T}_{p,q}$ bilden: Für jede Körpererweiterung K/k in einer vorgegebenen Kategorie von Körpererweiterungen $\mathfrak{G}(k)$ von k sind die Objekte von $\mathfrak{T}_K$ von der Form $((V,\delta),x)$, wobei V ein K-Vektorraum endlicher Dimension, $\delta : V \to V^*$ ein K-Isomorphismus und x ein Tensor vom Typ (p,q) auf V ist. Ein Morphismus $((V,\delta),x) \to ((V',\delta'),x')$ von Objekten von $\mathfrak{T}_K$ ist ein Homomorphismus von K-Vektorräumen $t : V \to V'$, so daß das Diagramm

$$\begin{array}{ccc} V & \xrightarrow{t} & V' \\ \delta \downarrow & & \downarrow \delta' \\ V^* & \xleftarrow{t^*} & V'^* \end{array},$$

in dem t^* den zu t dualen Homomorphismus bezeichnet, d.h. $t^*(h)(v) = h(t(v))$, $v \in V, h \in V'^*$, kommutiert, und so daß für den durch

$$V \xrightarrow{t} V' \text{ und } V^* \xrightarrow{\delta^{-1}} V \xrightarrow{t} V' \xrightarrow{\delta'} V'^*$$

induzierten Homomorphismus von K-Vektorräumen

$$\widetilde{t} : \otimes^p V \otimes \otimes^q V^* \to \otimes^p V' \otimes \otimes^q V'^*,$$

gilt

$$\widetilde{t}(x) = x'.$$

Sei L/K eine Körpererweiterung in $\mathfrak{G}(k)$, d.h. K, L sind Objekte von $\mathfrak{G}(k)$, so daß L/K eine Körpererweiterung ist. Setze $V_L := V \otimes_K L$. Jeder K-Isomorphismus $\delta : V \to V^*$ induziert den L-Isomorphismus

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$$\delta_L := \delta \otimes 1_L : V_L \to (V^*)_L = V_L^*,$$

d.h. $\delta_L(v \otimes \lambda) = \delta(v) \otimes \lambda$, $v \in V$, $\lambda \in L$,

und jeder Tensor x vom Typ (p,q) auf V definiert einen Tensor x_L vom Typ (p,q) auf V_L: Aus grundlegenden Eigenschaften des Tensorprodukts ergibt sich nämlich ein naheliegender Isomorphismus

$$\otimes_L^p V_L \otimes_L \otimes_L^q V_L^* \cong (\otimes_K^p V \otimes_K \otimes_K^q V^*) \otimes_K L,$$

und wir setzen

$$x_L := x \otimes 1_L.$$

Wenn keine Mißverständnisse zu befürchten sind, dann schreiben wir im Folgenden häufig auch $\delta_L = \delta$, $x_L = x$. Aus dem tensoriellen K-Objekt $((V,\delta),x)$ vom Typ (p,q) erhalten wir also das tensorielle L-Objekt $((V_L,\delta),x)$ vom Typ (p,q). Ist $t : ((V,\delta),x) \to ((V',\delta'),x')$ ein Morphismus von tensoriellen K-Objekten vom Typ (p,q), dann erhält man durch den Prozeß der Skalarerweiterung einen Morphismus $t_L : ((V_L,\delta_L),x_L) \to ((V'_L,\delta'_L),x_L)$ von tensoriellen L-Objekten.

Ist die Erweiterung L/K endlich und galoissch, dann erhält man für jedes tensorielle K-Objekt $((V,\delta),x)$ vom Typ (p,q) eine Anwendung der Galoisgruppe $G(L/K)$ auf das tensorielle L-Objekt $\otimes^p V_L \otimes \otimes^q V_L^*$: Die Anwendung auf V_L, also $s(v \otimes \lambda) := v \otimes s(\lambda)$, $s \in G(L/K), v \in V, \lambda \in L$, induziert eine Anwendung auf $V_L^* : s(f)(w) := s(f(s^{-1}(w))$, $s \in G(L/K)$, $f \in V_L^*$, $w \in V_L$. Damit erhält man eine Anwendung auf $\otimes^p V_L \otimes_L \otimes^q V_L^*$, und zwar durch

$$s((v_1 \otimes ... \otimes v_p) \otimes (f_1 \otimes ... \otimes f_q)) :=$$

$$:= (s(v_1) \otimes ... \otimes s(v_p)) \otimes (s(f_1) \otimes ... \otimes s(f_q)),$$

$$v_1, ..., v_p \in V_L, \;\; f_1, ..., f_q \in V_L^*.$$

Außerdem ist $s(\delta_L)(v \otimes \lambda) = s(\delta_L(s^{-1}(v \otimes \lambda))) = s(\delta(v) \otimes s^{-1}(\lambda)) = \delta(v) \otimes \lambda = \delta_L(v \otimes \lambda)$ für alle $s \in G(L/K), v \in V, \lambda \in L$, d.h.

$$s(\delta_L) = \delta_L \text{ für alle } s \in G(L/K),$$

und nach Konstruktion von x_L gilt

$$s(x_L) = x_L \text{ für alle } s \in G(L/K).$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Es folgt, daß $\mathfrak{T} = \mathfrak{T}_{\,p,q}$ eine Galois Kategorie ist, die durch die Kategorie $\mathfrak{G}(k)$ indiziert ist.

Für jedes K-Objekt $((V,\delta),x)$ von $\mathfrak{T}$ und jede Körpererweiterung L/K in $\mathfrak{G}(k)$ sei $E_{\mathfrak{T}}(L/K,((V,\delta),x))$ die Menge aller K-Isomorphieklassen $(((V',\delta'),x'))$ von K-Objekten $((V',\delta'),x')$ von $\mathfrak{T}$, die über L zu $((V,\delta),x)_L$ L-isomorph sind, d.h. für die ein Isomorphismus

$$((V,\delta),x)_L \to ((V',\delta'),x')_L$$

existiert, und sei

$$A_L := Aut((V,\delta),x)_L)$$

die Gruppe aller Automorphismen von $((V,\delta),x)_L$. Es gilt, vgl. $[SE1]$, Chapter X, §2, Proposition 4:

(2.1) **Satz** *Ist L/K eine endliche Galoiserweitrung in $\mathfrak{G}(k)$, dann ist die unter (1.6) definiert Abbildung*

$$\theta : E_{\mathfrak{T}_{p,q}}(L/K,((V,\delta),x)) \to H^1(G(L/K),A_L)$$

bijektiv.

Beweis: Aufgrund von (1.7) wissen wir, daß diese Abbildung injektiv ist. Um zu zeigen, daß sie im vorliegenden Fall auch surjektiv ist, gehen wir aus von einem 1-Kozykel

$$p : G \to A_L,\ s \mapsto p_s.$$

Wegen $A_L \subset GL(V_L)$ liefert das in (1.8) bewiesene Verschwinden von

$$H^1(G(L/K),GL(V_L))$$

einen L-Automorphismus $f : V_L \to V_L$ mit der Eigenschaft

$$p_s = f^{-1} \circ s(f) \ \text{ für alle } \ s \in G.$$

Sei

$$\widetilde{f} : \otimes^p V_L \otimes_L \otimes^q V_L^* \to \otimes^q V_L \otimes_L \otimes^q V_L^*$$

der durch f und $\delta : V \xrightarrow{\cong} V^*$ induzierte L-Automorphismus. Setze

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$x' := \widetilde{f}(x).$

Für $s \in G$ seien $\widetilde{s(f)}$ und $\widetilde{p_s}$ entsprechend definiert. x' ist rational über k, d.h. $x' \in \otimes^p V \otimes_k \otimes^q V^*$; denn für alle $s \in G$ gilt

$s(x') = s(\widetilde{f}(x)) = s(\widetilde{f})(s(x)) =$

$= s(\widetilde{f})(x)$, weil x K-rational ist, und

$s(\widetilde{f})(x) = \widetilde{s(f)}(x) =$

$= (\widetilde{f \circ p_s})(x) = (\widetilde{f} \circ \widetilde{p_s})(x) =$

$\widetilde{f}(x)$, weil $\widetilde{p_s}(x) = x$, und

$\widetilde{f}(x) = x'$,

insgesamt also $s(x') = x'$.

Somit ist $((V, \delta), x') \in E_{\mathfrak{T}}(L/K, ((V, \delta), x))$, und nach Konstruktion der Abbildung θ ist das Bild von $((V, \delta), x')$ unter θ gleich der vorgegebenen Kohomologieklasse $(p) \in H^1(G(L/K), A_K)$. Damit ist der Beweis von (2.1) beendet.

(2.2) **Beispiele** (a) Sei $\mathfrak{V}$ die Galoiskategorie der Vektorräume über einer Kategorie von Körpererweiterungen $\mathfrak{G}(k)$. In diesem Fall ist der Tensor $x = 0$, also vom Typ $(0, 0)$.

Für die beiden nachfolgenden Beispiele benötigen wir Aussagen über das Tensorprodukt von Vektorräumen, die z.B. in [$LG1$], Chapter XVI, insbesondere §2, bewiesen werden und die wir kurz wiederholgen. Seien dazu U, V, W endlichdimensionale K-Vektorräume, sei $L(U; V)$ der K-Vektorraum aller K-linearen Abbildungen $U \to V$ und sei $L^2(U, V; W)$ der K-Vektorraum aller K-bilinearen Abbildungen $U \times V \to W$. Dann existieren basisunabhängige Isomorphismen von K-Vektorräumen

$$L(U; L(V; W)) \cong L^2(U, V; W) \cong L(U \otimes V; W),$$

die wie folgt definiert sind: Der erste dieser Isomorphismen ordnet jeder K-linearen Abbildung $f : U \to L(V; W)$ die K-bilineare Abbildung $b_f : U \times V \to W$ mit

$$b_f(u, v) := f(u)(v), \;\; u \in U, \, v \in V,$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

zu, und der zweite dieser Isomorphismen ergibt sich aus der Konstruktion des Tensorprodukts. Ist L/K eine Körpererweiterung, dann induzieren diese Isomorphismen entsprechende Isomorphismen von L-Vektorräumen, die für den Fall, daß L/K eine endliche Galoiserweiterung ist, jeweils mit der Operation der Galoisgruppe $G = G(L/K)$ verträglich sind:

$$L \otimes_K L(U; L(V; W)) \cong L(U_L; L(V_L; W_L)) \cong$$

$$L^2(U_L, V_L; W_L) \cong L \otimes_K L^2(U, V; W) \cong$$

$$L \otimes_K L(U \otimes V; W) \cong L(U_L \otimes_K V_L; W_L).$$

(b) (Vgl. $[SE1]$, Chapter X, §2) In diesem Beispiel nehmen wir an, daß die Charakteristik des Körpers k nicht 2 ist. Sei K/k eine Körpererweiterung in einer Kategorie von Körper- erweiterungen $\mathfrak{G}(k)$ von k und sei $q : V \to K$ eine nichtausgeartete quadratische Form auf dem endlichdimensionalen K-Vektorraum V. Sei

$$b_q : V \times V \to K$$

die zugehörige nichtausgeartete symmetrische Bilinearform, d.h.

$$b_q(v_1, v_2) = \frac{1}{2}(q(v_1 + v_2) - q(v_1) - q(v_2))$$

Wegen $L^2(V, V; K) \cong L(V \otimes V; K) \cong V^* \otimes V^*$ entspricht b_q einem Tensor x vom Typ $(0, 2)$ auf V, und für jede Körpererweiterung L/K in $\mathfrak{G}(k)$ ist

$$E_{\mathfrak{T}_{0,2}}(L/K, ((V, \delta), x)),$$

wobei $\delta : V \cong V^*$ der durch $V \to V^*, v \mapsto b(v, -)$, gegebene Isomorphismus ist, die Menge der K-Isomorphieklassen $E(L/K, (V, q)) = E_{\mathfrak{T}_{0,2}}(L/K, ((V, \delta), x)$ aller nichtausgearteten quadratischen Räume (V', q'), die über L isomorph zu $(V, q)_L$ sind, d.h. für die ein L-Isomorpismus $f : V_L \to V'_L$ existiert, so daß

$$b_{q'}(f(v), f(w)) = b_q(v, w) \text{ für alle } v, w \in V_L.$$

Ist L/K endlich und galoissch, so ist die Gruppe aller L-Automorphismen von $((V, \delta), x)_L$ aufgrund der obigen Vorbemerkung $G(L/K)$-isomorph zur orthogonalen Gruppe $O_L(q)$ von $(V, q)_L$ über L. Nach (1.7) und (2.1) ist die Abbildung.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$$E(L/K,(V,q)) \to H^1(G(L/K),O_L(q)),$$

die der unter (1.6) definierten Abbldung θ entspricht, bijektiv.

(c) (Vgl. [*SE*1], Chapter X, §5) Sei R ein kommutativer Ring mit 1. Eine R-Algebra ist ein Paar (A,α), wobei A ein R-Modul und $\alpha : A \times A \to A$ eine R-bilineare Abbildung ist. Ein Homomorphismus von R-Algebren $f : (A,\alpha) \to (B,\beta)$ ist eine R- lineare Abbildung $f : A \to B$ mit der Eigenschaft $\beta(f(a),f(a')) = f(\alpha(a,a'))$ für alle $a,a' \in A$. Häufig betrachten wir nur spezielle R-Algebren A, die auf folgende Weise entstehen: A ist ein assoziativer Ring und $f : R \to A$ ist ein Ringhomomorphismus, so daß $f(R)$ im Zentrum von A enthalten ist. Dann wird A durch die Festsetzung $R \times A \to A$, $(r,a) \longmapsto f(r)a$ zu einem R-Modul, und die Ringmultiplikation $A \times A \to A$ ist R-bilinear. Ist $R = K$ ein Körper und (V,α) eine endlichdimensionale K-Algebra , so wird die zugehörige K-bilineare Abbildung $\alpha : V \times V \to V$ wegen $L^2(V,V;V) \cong V \otimes_k V^* \otimes_k V^*$ durch einen Tensor x vom Typ $(1,2)$ auf V beschrieben. Ist L/K eine Körpererweiterung in einer Kategorie von Körpererweiterungen $\mathfrak{G}(k)$ von k, dann ist für jedes K-Objekt $((V,\delta),x)$ der k-Kategorie $\mathfrak{T}_{1,2}$ die Menge $E_{\mathfrak{T}_{1,2}}(L/K,((V,\delta),x))$ bijektiv zur Menge $E(L/K,(V,\alpha))$ der K-Isomorphieklassen endlichdimensionaler K-Algebren (V',α'), die über L isomorph zu $(V,\alpha)_L$ sind, d.h. für die ein L-Isomorphismus $f : V_L \to V'_L$ existiert, so daß

$$\alpha'(f(v),f(w)) = f(\alpha(v,w)) \quad \text{für alle } v,w \in V_L.$$

Ist also L/K eine endliche Galoiserweiterung und $A_L((V,\alpha))$ die Gruppe aller L-Automorphismen von $(V,\alpha)_L$, so ist nach (1.7) und (2.1) die Abbildung

$$E(L/K,(V,\alpha)) \to H^1(G(L/K),A_L((V,\alpha))),$$

die der unter (1.6) definierten Abbldung θ entspricht, bijektiv.

(d) In dem Fall, daß die Charakteristik von k gleich 2 ist, lassen sich quadratische Formen über k bekanntlich nicht alle durch symmetrische Bilinearformen beschreiben. Für quadratische Formen über einem beliebigen Körper wählt man daher zu ihrer kohomologischen Beschreibung einen direkten Weg. Wir erläutern kurz die dafür nötigen Begriffe und verweisen für die Einzelheiten auf die grundlegende Arbeit [*SR*]. Sei dazu k ein beliebiger Körper und sei K/k eine Körpererweiterung in einer Kategorie von Körpererweiterungen $\mathfrak{G}(k)$ von k. Eine quadratische Form auf einem n-dimensionalen K-Vektorraum V ist eine Abbildung $q : V \to K$ mit $q(\alpha v) = \alpha^2 q(v)$ für alle $\alpha \in K$ und alle $v \in V$ und mit der Eigenschaft, daß die Abbildung $b := b_q : V \times V \to K$, $b(v,w) := q(v+w) - q(v) - q(w)$, bilinear ist. Wir nehmen nachfolgend stets an, daß b_q nichtausgeartet ist; das Paar (V,q) heißt dann auch *quadratischer Raum über K*. Ein Morphismus von einem quadratischen Raum (V,q) in den quadratischen Raum (V',q') ist ein Homomorphismus von K-Vektorräumen $f : V \to V'$ mit der Eigenschaft $q' \circ f = q$. Sei L/K eine Körpererweiterung in $\mathfrak{G}(k)$. Dann ist durch

$q_L(\sum_{i=1}^n v_i \otimes \lambda_i) := \sum_{i=1}^n \lambda_i^2 q(v_i) + \sum_{i<j} \lambda_i \lambda_j b_q(v_i, v_j)$,

$\lambda_i \in L$, $v_i \in V$, eine quadratische Form $q_L : V_L \to L$ auf dem L-Vektorraum $V_L = V \otimes_K L$ definiert. Mit q ist auch q_L nichtausgeartet.

Sei L/K eine endliche Galoiserweiterung in $\mathfrak{G}(k)$ und sei (V, q) ein quadratischer Raum über K. Die durch $G(L/K) \times V_L \to V_L$, $(s, v \otimes \lambda) \mapsto v \otimes s(\lambda)$, erklärte Anwendung von $G(L/K)$ auf V_L induziert eine Anwendung von $G(L/K)$ auf der Menge aller Abbildungen $\varphi : V_L \to L$:

$s(\varphi)(w) := s(\varphi(s^{-1}(w)))$, $s \in G(L/K)$, $w \in V_L$.

Aus der obigen Definition von q_L folgt daher

$s(q_L) = q_L$ für alle $s \in G(L/K)$.

Mit diesen Festsetzungen und Bemerkungen folgt, daß die quadratischen Räume über Körpererweiterungen von k eine Galoiskategorie über $\mathfrak{G}(k)$ bilden. Man zeigt unter Benutzung von (1.8), daß auch in diesem Fall die Abbildung

$\theta : E(L/K, (V, q)) \to H^1(G(L/K), Aut((V, q)_L))$

nicht nur injektiv sondern auch surjektiv ist.

Aufgaben und Beispiele

(1) Wiederholen Sie die Konstruktion sowie die universelle Eigenschaft des Tensorprodukts von Moduln und Algebren. Erarbeiten Sie außerdem den Begriff der Tensoralgebra. (Vgl. z.B. [$LG1$], Chapter XVI, §5, oder [CH])

(2) Sei L/K eine endliche Galoiserweiterung mit Galoisgruppe G. Sei (V, q) ein nichtausgearteter quadratischer Raum über K. Zeigen Sie, daß die unter (1.6) definierte Abbildung $E(L/K, (V, q)) \to H^1(G, Aut((V, q)_L))$ surjektiv ist. (Vgl. [SR])

§ 3. Prinzipale homogene Räume

In diesem Abschnitt wird die 1-te Kohomologiemenge $H^1(G, A)$ mit Hilfe sogenannter prinzipaler homogener Räume beschrieben. Dabei folgen wir [$SE2$], Chapter I, §5, 5.2.

Sei G eine Gruppe und sei E eine Links-G-Menge. Es existiert also eine Abbildung $G \times E \to E$, $(s, x) \mapsto s(x) = x^s$, so daß $s(t(x)) = st(x)$, $e_G(x) = 1$ für alle $x \in E$ und alle $s, t \in G$. Sei außerdem A eine Links-G-Gruppe. Man sagt, daß A von rechts auf E in einer mit der Operation von G auf A verträglichen Weise operiert, wenn A von rechts auf E operiert und wenn gilt

$s(xa) = s(a)s(x)$ für alle $s \in G$, $a \in A$, $x \in E$.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Mit anderen Worten: Die Abbildung $E \times A \to E$, die der Rechtsoperation von A auf E entspricht, ist ein G-Morphismus. Operiert A in dieser Weise von rechts auf E, so schreibt man für E auch E_A. Ähnliche Festsetzungen macht man, wenn A von links auf E operiert und schreibt dann für E auch ${}_AE$.

Definition Ein *prinzipaler homogener G-Raum für A* ist eine nichtleere Links-G-Menge P, so daß A in einer mit der Operation von G verträglichen Weise von rechts auf P operiert, und zwar so, daß P eine affine Menge ist, d.h. zu je zwei Elementen $x, y \in P$ existiert genau ein $a \in A$, so daß $y = xa$. Zwei prinzipale homogene Räume P, P' für A heißen *isomorph*, falls eine bijektive G-equivariante Abbildung $P \to P'$ existiert, so daß das folgende Diagramm kommutiert

$$\begin{array}{ccccc} P & \times & A & \to & P \\ \downarrow & & & & \downarrow \\ P' & \times & A & \to & P' \end{array}$$

Man erhält auf diese Weise eine Aequivalenzrelation.

Sei $\mathcal{P}(G, A)$ die entsprechende Menge von Isomorphieklassen (P) prinzipaler homogener Räume P für A.

(3.1) **Satz** (Vgl. [$SE2$], Chapter I, §5, 5.2, Proposition 33) *Sei A eine Links G-Gruppe. Dann existiert eine bijektive Abbildung*

$$\lambda : \mathcal{P}(G, A) \to H^1(G, A).$$

Beweis: Sei $(P) \in \mathcal{P}(G, A)$ und sei $x \in P$. Für alle $s \in G$ ist $s(x) \in P$. Also existiert genau ein $a_s \in A$, so daß $s(x) = xa_s$. Die Abbildung

$$\alpha_P = \alpha : G \to A,\ s \mapsto a_s$$

ist ein 1-Kozykel: $st(x) = s(t(x)) = s(xa_t) = s(x)s(a_t) = xa_s s(a_t) = xa_{st}$. Nimmt man xb mit $b \in A$ an Stelle von x, so ändert sich der durch x definierte 1-Kozykel α zu $s \mapsto b^{-1}a_s b^s$; denn $(xb)b^{-1}a_s b^s = xa_s b^s = s(x)s(b) = s(xb)$. Der durch xb definierte 1-Kozykel ist also aequivalent zu dem durch x definierten 1-Kozykel. Somit ist durch

$$\lambda((P)) := \text{Kozykelklassse von } \alpha$$

eine Abbildung $\lambda : \mathcal{P}(G, A) \to H^1(G, A)$ wohldefiniert. Man erhält zu λ folgendermaßen eine Umkehrabbildung

$$\mu : H^1(G, A) \to \mathcal{P}(G, A) :$$

Sei $\alpha : G \to A$, $s \mapsto a_s$, ein 1-Kozykel. Sei P_α die Menge, die dieselben Elemente wie A enthält, und auf der G von links durch

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$s\,[x] := a_s s(x),\ s \in G,\ x \in P_a$

und auf der A von rechts durch Rechtsmultiplikation (Translation)

$[x]\,a := xa,\ a \in A,\ x \in P_a,$

operiert. ($e_G[x] = x$ wegen $a_{e_G} = 1$ und $s[t[x]] = s\,[a_t t(x)] = a_s s(a_t t(x)) = a_s s(a_t) st(x) = a_{st} st(x) = st\,[x]$.) Auf diese Weise wird P_a zu einem prinzipalen homogenen Raum für A. Zwei aequivalente 1-Kozykeln ergeben nach dieser Konstruktion isomorphe prinzipale homogene Räume für A. Man definiert daher

$\mu((\alpha)) := (P_\alpha).$

μ ist die Umkehrabbildung für λ. Damit ist der Beweis von (3.1) beendet.

(3.2) **Beispiele** (a) (Vgl. [*SE*2], Chapter III, §1, 1.1) Sei K/k eine Körpererweiterung in einer Kategorie von Körpererweiterungen $\mathfrak{G}(k)$ von k, sei V ein endlichdimensionaler K-Vektorraum, versehen mit einem Isomorphismus $\delta : V \to V^*$, und sei x ein Tensor vom Typ (p, q) auf V. $((V, \delta), x)$ ist also ein K-Objekt aus der in § 2 definierten Kategorie $\mathfrak{T} = \mathfrak{T}_{p,q}$. Sei L/K eine endliche Galoiserweiterung in $\mathfrak{G}(k)$, sei $((V', \delta'), x')$ eine L/K-Form von $((V, \delta), x)$ und sei P die Menge aller L-Isomorphismen von $((V'_L, \delta'), x')$ nach $((V_L, \delta), x)$. P ist ein prinzipaler homogener Raum für die Automorphismengruppe A_L von $((V_L, \delta), x)$: A_L operiert durch Verknüpfung mit Automorphismen von rechts auf P. Diese Operation ist mit der Linksoperation der Galoisgruppe $G = G(L/K)$ auf P verträglich. Außerdem ist die Operation von A_L auf P affin. Die Zuordnung $((V', \delta'), x') \mapsto P$ induziert eine Abbildung

$\mu : E_{\mathfrak{T}_{p,q}}(L/K, ((V, \delta), x)) \to \mathcal{P}(G, A_L),$

aus der sich aufgrund von (3.1) und der Bijektion (2.1) die bijektive Abbildung

(3.3) $\mu \circ \theta : H^1(G, A_L) \to \mathcal{P}(G, A_L)$

ergibt.

(b) Seien $a \in \mathbb{Q}^* \setminus \{\pm 1\}$ und $n \in \mathbb{N}$, $n \geq 2$, so, daß das Polynom $f := X^n - a \in \mathbb{Q}\,[X]$ irreduzibel ist. Sei P die Menge aller Nullstellen von f in $\mathbb{C}$ und K der Teilkörper von $\mathbb{C}$, der aus $\mathbb{Q}$ durch Adjunktion aller Elemente aus P entsteht. K ist ein Zerfällungskörper von f. Sei $G = G(K/\mathbb{Q})$ die entsprechende Galoisgruppe von $K/\mathbb{Q}$. P ist eine G-Menge. Es folgt, daß die G-Gruppe $A := \mu_n :=$ Gruppe aller $n-$ten Einheitswurzeln in $\mathbb{C}$ durch Multiplikation G-verträglich auf P operiert und daß P dadurch zu einem prinzipalen homogenen G-Raum für A wird. Die zugehörige Klasse $(P) \in \mathcal{P}(G, A)$ entspricht aufgrund von (3.1) genau einem Element $\lambda((P)) \in H^1(G, A)$, das sich durch den $1-$Kozykel $\alpha : G \to A$, $s \mapsto s(x)/x$, wobei x irgendein Element aus P ist, repräsentieren läßt.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

(3.4) **Twistung** (vgl. [$SE2$], Chapter I, §5, 5.3) Sei G eine Gruppe, sei A eine Links-G-Gruppe und sei P ein prinzipaler homogener G-Raum für A. Sei F eine Links-G-Menge, auf der A G-verträglich von links operiert. Auf dem cartesischen Produkt $P \times F$ definieren wir wie folgt eine Aequivalenzrelation: $(p, f), (p', f') \in P \times F$ heißen aequivalent, wenn ein $a \in A$ existiert, so daß $(p', f') = (pa, a^{-1}f)$ Diese Aequivalenzrelation ist mit der Operation von G verträglich, so daß also die Menge aller Aequivalenzklassen eine G-Menge ist, die mit $P \times^A F$ oder ${}_PF$ bezeichnet wird. Jedes Element aus ${}_PF$ ist von der Form pf mit $p \in P$ und $f \in F$, und es gilt $(pa)f = p(af)$ für alle $a \in A$. Außerdem ist für jedes $p \in P$ die Abbildung $F \to {}_PF$, $f \mapsto pf$, bijektiv.

Definition $P\times {}^AF = {}_PF$ heißt *Twistung von F mit P*

Diese Twistung läßt sich mit Hilfe des 1-Kozykels $\alpha : G \to A$, $s \mapsto a_s$, beschreiben, der zu P gehört, d.h. für den $s(p) = pa_s$ für alle p$\in P$ gilt. ${}_\alpha F$ sei die Links-G-Menge, die als Menge mit F übereinstimmt und auf der G wie folgt operiert:

$$G\times {}_\alpha F \xrightarrow{\kappa} {}_\alpha F, \ \ (s, f) \mapsto a_s s(f).$$

Es folgt, daß für jedes $p \in P$ die Abbildung

$${}_\alpha F \to {}_PF, \ f \mapsto pf,$$

ein Isomorphismus von G-Mengen ist $(p\kappa((s, f)) = pa_s s(f) = s(p)s(f) = s(pf))$; und wenn P aequivalent zu P' mit entsprechenden aequivalenten 1-Kozykeln α, α' ist, dann sind ${}_PF$ und ${}_{P'}F$ bzw. ${}_\alpha F$ und ${}_{\alpha'}F$ isomorph.

Für weitere Bemerkungen über Twistungen vgl. man [$SE2$], Chapter I, §5, 5.3.

Aufgaben und Beispiele

(1) Geben Sie ausführliche Beweise für alle im Beispiel (3.2), (b) gemachten Aussagen.

(2) Sei L/K eine endliche Galoiserweiterung mit der Galoisgruppe G und sei $N : L^* \to K^*$ der Normhomomorphismus. N ist eine G-equivariante Abbildung. Sei L^N der Kern von N. Die exakte G-Sequenz

$$1 \to L^N \to L^* \xrightarrow{N} N(L^*) \to 1$$

induziert daher nach (1.5) die exakte Sequenz

$$1 \to H^0(G, L^N) \to H^0(G, L^*) \xrightarrow{N} H^0(G, N(L^*)) \xrightarrow{\delta} H^1(G, L^N) \to H^1(G, L^*)$$

Nach (1.8) ist $H^1(G, L^*) = 1$. Außerdem ist $H^0(G, L^*) = K^*$ und

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$H^0(G, N(L^*)) = N(L^*)$, $N(K^*) = K^{*n}$ mit $n = (L : K)$. Also

$$N(L^*)/K^{*n} \overset{\delta}{\cong} H^1(G, L^N).$$

Nach Definition von δ und der Deutung von $H^1(G, L^N)$ durch prinzipale homogene G-Räume für L^N entspricht δ der Abbildung

$$a \bmod K^{*n} \mapsto (P_a), \text{ wobei } P_a := \{x \in L^* : N(x) = a\}. \text{ (Wohlbekannt)}$$

§ 4. Gruppenerweiterungen und Kozykeln

In diesem Abschnitt werden Zusammenhänge zwischen Gruppenerweiterungen und Kozykeln erläutert. Für ausführlichere Darstellungen verweisen wir auf entsprechende Abschnitte in Lehrbüchern über Gruppenkohomologie, z.B. [$LG2$], sowie auf [AT], Chapter XIII.

Sei G eine Gruppe und sei A ein G-Modul, d.h. eine kommutative - multiplikativ geschriebene - Gruppe, auf der G von links durch Gruppenautomorphismen operiert: $G \times A \to A$, $(s, a) \mapsto s(a) = a^s$. Sei $Z^2(G, A)$ die Menge aller 2-Kozykeln von G in A, d.h. aller Abbildungen

$$f : G \times G \to A,\ (s, t) \mapsto f(s, t) = f_{s,t}$$

mit der Eigenschaft

$$r(f_{s,t})f_{r,st} = f_{r,s}f_{rs,t} \quad \text{für alle} \quad r, s, t \in G.$$

$Z^2(G, A)$ ist bezüglich der punktweise definierten Multiplikation eine kommutative Gruppe. Sei $B^2(G, A)$ die Untergruppe von $Z^2(G, A)$, die aus allen 2-Korändern $f : G \times G \to A$ besteht, d.h. zu f existiert eine Abbildung $\lambda : G \to A$, $s \mapsto \lambda(s) = \lambda_s$, so daß $f_{s,t} := (\delta\lambda)_{s,t} := \lambda_s s(\lambda_t)/\lambda_{st}$ für alle $s, t \in G$.

Definition Die Faktorgruppe

$$H^2(G, A) := Z^2(G, A)/B^2(G, A)$$

heißt die *2-te Kohomologiegruppe von G mit Koeffizienten in A*; ihre Elemente (f) heißen *2-Kozykelklassen von G in A*.

Eine Gruppenerweiterung von G mit dem Kern A, wobei A eine - nicht notwendigerweise kommutative - Gruppe ist, ist eine Gruppe E zusammen mit einer exakten Sequenz von Gruppenhomomorphismen der Form

$$1 \to A \to E \to G \to 1.$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Zwei Gruppenerweiterungen E, E' von G mit dem abelschen Kern A heißen *aequivalent*, wenn ein Isomorphismus $F : E \to E'$existiert, so daß das folgende Diagramm kommutiert

$$\begin{array}{ccccccccc} 1 & \to & A & \to & E & \to & G & \to & 1 \\ & & \downarrow id & & \downarrow F & & \downarrow id & & \\ 1 & \to & A & \to & E' & \to & G & \to & 1. \end{array}$$

Dadurch ist auf der Menge aller Gruppenerweiterungen von G mit dem abelschen Kern A eine Aequivalenzrelation definiert. Sei $\mathcal{E}(G, A)$ die Menge dieser Aequivalenzklassen.

(4.1) **Satz** *Ist A abelsch, dann gibt es eine bijektive Abbildung*

$$H^2(G, A) \to \mathcal{E}(G, A).$$

Diese bijektive Abbildung entsteht wie folgt: Ist $f : G \times G \to A$ ein 2-Kozykel, so bildet man

$$E := G(f) := \{(a, s) : a \in A,\ s \in G\}$$

und definiert für zwei Elemente $(a, s), (b, t) \in G(f)$ deren Verknüpfung durch

$$(a, s)(b, t) := (as(b)f_{s,t}, st).$$

Dadurch wird E zu einer Gruppe; das neutrale Element dieser Gruppe ist

$$(f_{1,1}^{-1}, 1)$$

und das zu (a, s) inverse Element ist

$$(s^{-1}(a^{-1})f_{s^{-1},s}^{-1}f_{1,1}^{-1}, s^{-1}).$$

Man identifiziert A mit der Untergruppe von $G(f)$, die aus allen Elementen der Form $(af_{1,1}^{-1}, 1)$, $a \in A$, besteht. Die Abbildung $E \to G$, $(a, s) \mapsto s$, ist ein surjektiver Gruppenhomomorphismus mit dem Kern A. E ist also eine Gruppenerweiterung von G mit dem Kern A. Ist $f := f'(\delta\lambda)$, wobei $\delta\lambda$ den zur Abbildung $\lambda : G \to A$, $s \mapsto \lambda_s$, gehörigen Korand bezeichnet, dann ist

$$F : G(f) \to G(f'),\ (a, s) \mapsto (a\lambda_s, s)$$

ein Isomorphismus, der eine Aequivalenz der entsprechenden Gruppenerweiterungen $E = G(f)$ und $E' = G(f')$ von G mit dem Kern A bewirkt.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Sei umgekehrt $1 \to A \to E \xrightarrow{p} G \to 1$ eine Gruppenerweiterung von G mit dem Kern A und sei $u : G \to E$ ein Schritt zu p. Dann ist die Abbildung

$$f : G \times G \to A, \ \ (s,t) \mapsto f_{s,t} := u_s u_t u_{st}^{-1}$$

aufgrund des in E geltenden Assoziativgesetzes ein 2-Kozykel. Ist E vermöge des Isomorphismus $F : E \to E'$ aequivalent zur Gruppenerweiterung E' von G mit dem Kern A, dann ist $u' := F \circ u : G \to E'$ ein Schnitt zu dem gegebenen Epimorphismus $p' : E' \to G$. Also existiert eine Abbildung $\lambda : G \to A$, so daß $u'_s = \lambda_s u_s$ und damit $f'_{s,t} := u'_s u'_t u'^{-1}_{st} = (\delta\lambda)_{s,t} f_{s,t}$ für alle $s, t \in G$.

Insgesamt ist damit gezeigt, daß die Abbildung

$$H^2(G,A) \to \mathcal{E}(G,A), \ (f) \mapsto (G(f))$$

von der Gruppe $H^2(G,A)$ aller 2-Kozykelklassen von G in A in die Menge $\mathcal{E}(G,A)$ aller Aequivalenzklassen von Gruppenerweiterungen von G mit Kern A bijektiv ist.

Die dadurch auf $\mathcal{E}(G,A)$ induzierte Gruppenstruktur ist gegeben durch das sogenannte *Baer-Produkt*: Sind $(E), (E') \in \mathcal{E}(G,A)$ mit entsprechenden Epimorphismen $p : E \to G$, $p' : E' \to G$ und mit entsprechenden Kozykelklassen $(f), (f') \in H^2(G,A)$, dann ist dieses Produkt gegeben durch

$$(E) \cdot (E') := ((E \times_G E')/D(A)),$$

wobei

$$E \times_G E' := \{(e,e') \in E \times E' : p(e) = p'(e')\}$$

das entsprechende Faserprodukt über G und $D(A)$ die durch

$$D(A) := \{(a,b) \in A \times A : a = b^{-1}\}$$

definierte Untergruppe von $A \times A$ ist. Die Abbildung $E \times_G E' \to G$, $(e,e') \mapsto p(e) = p'(e')$, ist ein Epimorphismus, dessen Kern die Gruppe $A \times A$, also auch die Gruppe $D(A)$, enthält, und die Abbildung $A \times A \to A$, $(a,b) \mapsto ab$, ist ein Epimorphismus mit dem Kern $D(A)$. Man hat also eine Gruppenerweiterung

$$1 \to A \to (E \times_G E')/D(A) \to G \to 1.$$

Die Aequivalenzklasse dieser Gruppenerweiterung entspricht unter der in (4.1) gegebenen Korrespondenz dem Produkt der entsprechenden Kozykelklassen; vgl. dazu z.B. $[MAL]$, p. 69 ff.

Nachfolgend machen wir gelegentlich Gebrauch von der Tatsache, daß jeder G-Homomorphismus $f : A \to A'$ von G-Moduln, d.h. jeder Homomorphismus $f : A \to A'$ mit der Eigenschaft $f(s(a)) = s(f(a))$ für alle $a \in A$, $s \in G$, den Homomorphismus

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$f_* = f_2 : H^2(G, A) \to H^2(G, A'),\ (c) \mapsto (f_*(c)),$

induziert, wobei

$f_*(c)(s,t) := f(c(s,t)),\ \ s, t \in G.$

Außerdem benutzen wir häufig, daß jeder Gruppenhomomorphismus $\varphi : G \to G'$ den Homomorphismus

$\varphi^* : H^2(G', A) \to H^2(G, A),\ \ (c) \mapsto (\varphi^*(c)),$

induziert, wobei

$\varphi^*(c)(s,t) := c(\varphi(s), \varphi(t)),\ \ s, t \in G.$

Gruppenerweiterungen mit abelschem Kern, d.h. exakte Sequenzen von Gruppenhomomorphismen $1 \to A \to E \xrightarrow{p} G \to 1$ mit abelscher Gruppe A, bilden die Objekte einer Kategorie. Die Morphismen in dieser Kategorie sind Tripel von Gruppenhomomorphismen

$(f : A \to A', F : E \to E', \varphi : G \to G'),$

so daß das folgende Diagramm kommutiert

$$\begin{array}{ccccccccc} 1 & \to & A & \to & E & \xrightarrow{p} & G & \to & 1 \\ & & f \downarrow & & F \downarrow & & \varphi \downarrow & & \\ 1 & \to & A' & \to & E' & \xrightarrow{p'} & G' & \to & 1\ . \end{array}$$

In [AT], Chapter XIII, wird das folgende Resultat bewiesen.

(4.2) **Satz** *Seien $1 \to A \to E \xrightarrow{p} G \to 1$, $1 \to A' \to E' \xrightarrow{p'} G' \to 1$ Gruppenerweiterungen mit abelschen Gruppen A, A' und seien $f : A \to A'$, $\varphi : G \to G'$ Homomorphismen. Dann existiert ein Homomorphismus $F : E \to E'$, so daß das Tripel (f, F, φ) genau dann ein Morphismus der gegebenen Gruppenerweiterung ist, wenn die beiden folgenden Bedingungen erfüllt sind:*

(i) *f ist ein G-Homomorphismus, wobei G auf A' über φ operiert*

(ii) *$f_*((c)) = \varphi^*((c'))$, wobei $(c) \in H^2(G, A)$ bzw. $(c') \in H^2(G', A')$ im Sinne von (4.1) zu E bzw. E' gehört und*

$f_* : H^2(G, A) \to H^2(G, A')$

der durch den G-Homomorphismus $f : A \to A'$ und

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$$\varphi^* : H^2(G', A') \to H^2(G, A')$$

der durch den Homomorphismus $\varphi : G \to G'$ *induzierte Homomorphismus ist.*

Zwei Homomorphismen $F, F' : E \to E'$, so daß die Tripel

$$(f : A \to A', F : E \to E', \varphi : G \to G')$$

und

$$(f : A \to A', F' : E \to E', \varphi : G \to G')$$

Morphismen von Gruppenerweiterungen sind, heißen aequivalent, wenn ein $a' \in A'$ existiert, so daß

$$F'(e) = a'F(e)a'^{-1} \text{ für alle } e \in E.$$

Hierdurch wird eine Aequivalenzrelation definiert; wir bezeichnen die entsprechende Menge von Aequivalenzklassen mit $\mathcal{F}$. Auch die folgende Aussage wird in $[AT]$, Chapter XIII, bewiesen.

(4.3) **Zusatz** *Die Gruppe* $H^1(G, A')$ *operiert folgendermaßen transitiv und fixpunktfrei auf* $\mathcal{F}$:

$$H^1(G, A') \times \mathcal{F} \to \mathcal{F}, \;\; ((\gamma), (F)) \mapsto (\gamma F),$$

wobei

$$(\gamma F)(au_s) := f(a)\gamma(s)F(u_s), \; a \in A, \; s \in G$$

mit einem Repräsentantensystem $u_s, s \in G$, *von* G *in* E.

Sei $N \trianglelefteq G$ ein Normalteiler der Gruppe G und sei A eine - nicht notwendigerweise kommutative - G-Gruppe. Dann operiert die Faktorgruppe G/N auf der Gruppe $H^0(N, A) = A^N$. Also ist die Kohomolgiemenge $H^1(G/N, A^N)$ definiert. G operiert auch auf der Kohomologiemenge $H^1(N, A)$:

$$G \times H^1(N, A) \to H^1(N, A), \; (s, (\alpha)) \mapsto (s(\alpha)),$$

wobei $s(\alpha)(n) := s(\alpha(s^{-1}ns)), \quad n \in N, s \in G$. Es folgt, daß N trivial operiert:

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$n^{'}(\alpha)(n) = n'(\alpha(n'^{-1}nn')) = n'(\alpha(n'^{-1})n'^{-1}(\alpha(nn'))) = n'(\alpha(n'^{-1})\alpha(nn') = \alpha(n')^{-1}\alpha(n)n((\alpha(n'))$ für alle $n, n' \in N$.

Ist $\alpha : G/N \to A^N$ ein 1-Kozykel, so ist

$inf(\alpha) : G \to A, \;\; inf(\alpha)(s) := \alpha(sN), \quad s \in G,$

ebenfalls ein 1-Kozykel. Dadurch erhält man die sogenannte Inflationsabbildung

$inf : H^1(G/N, A^N) \to H^1(G, A);$

sie bildet das ausgezeichnete Element auf das ausgezeichnete Element ab. Außerdem erhält man durch Einschränkung des Definitionsbereichs jedes 1-Kozykels $\alpha : G \to A$ auf N eine Abbildung

$res : H^1(G, A) \to H^1(N, A)^{G/N}.$

Durch direktes Nachrechnen bestätigt man den folgenden wohlbekannten Satz.

(4.4) **Satz** *Sei G eine Gruppe, sei $N \trianglelefteq G$ ein Normalteiler und sei A eine G-Gruppe. Dann ist die nachfolgende Sequenz von Abbildungen punktierter Kohomologiemengen exakt*

$1 \to H^1(G/N, A^N) \overset{inf}{\to} H^1(G, A) \overset{res}{\to} H^1(N, A)^{G/N}.$

Wir fragen nun, ob man für eine kommutative G-Modul A die vorstehende exakte Sequenz in geeigneter Weise nach rechts ausdehnen kann und berichten über ein entsprechendes Resultat aus [HS], Chapter III, section 4, das diese Frage beantwortet.

A sei also eine kommutative G-Gruppe. N sei weiterhin ein Normalteiler von G. Ist N' die Kommutatorgruppe von N, dann ist N' ein Normalteiler von G, und

$1 \to N/N' \to G/N' \to G/N \to 1$

ist eine Gruppenerweiterung mit dem abelschen Kern N/N'. Sei

$(c) \in H^2(G/N, N/N')$

die zugehörige Kozykelklasse (vgl. (4.1)). (c) definiert den sogenannten *Transgressionshomomorphismus*

$\tau = \tau_{(c)} : H^1(N, A)^{G/N} \to H^2(G/N, A^N), \; (\alpha) \mapsto (\tau(\alpha)),$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

wobei

$$\tau(\alpha)(s,t) := \alpha(n(c(s,t))); \quad s,t \in G/N,$$

mit einem Schnitt $n : N/N' \to N$. Außerdem erhält man den Inflationshomomorphismus

$$inf = \inf^G_{G/N} : H^2(G/N, A^N) \to H^2(G,A),\ (f) \mapsto (\inf(f)),$$

$$inf(f)(s,t) := f(sN, tN), \quad s,t \in G.$$

Das folgende Resultat, das häufig durch Anwendung von Spektralsequenzen bewiesen wird, vgl.[HS], Chapter III, section 4, oder [$LG2$], Chapter III, läßt sich auch durch direktes Nachrechnen überprüfen; vgl. dazu auch [H].

(4.5) **Satz** *Sei G eine Gruppe, sei $N \trianglelefteq G$ ein Normalteiler und sei A eine abelsche G-Gruppe. Dann ist die nachfolgende Sequenz von Homomorphismen abelscher Gruppen exakt*

$$1 \to H^1(G/N, A^N) \overset{inf}{\to} H^1(G,A) \overset{res}{\to} H^1(N,A)^{G/N} \overset{\tau}{\to}$$

$$\overset{\tau}{\to} H^2(G/N, A^N) \overset{inf}{\to} H^2(G,A).$$

Für die nachfolgenden Konstruktionen vgl. [$SE1$], Chapter VII, Appendix) Sei G eine Gruppe und sei

$$1 \to A \overset{i}{\to} B \overset{p}{\to} C \to 1$$

eine exakte Sequenz von G-Gruppen. Wir erinnern an die Korandabbildung $\delta : H^0(G,C) \to H^1(G,A)$ aus §1: Sei $c \in C^G$. Sei $b \in B$ so, daß $p(b) = c$. Dann ist $b^{-1}s(b) \in i(A)$ für alle $s \in G$ $(p(s(b)) = s(p(b)) = s(c) = c = p(b))$. Wir definieren eine Abbildung

$$\alpha : G \to A,\ s \mapsto \alpha(s) := a_s := i^{-1}(b^{-1}(s(b))),$$

und stellen fest, daß dadurch ein 1-Kozykel definiert wird. Mit der vereinfachten Schreibweise $i(a) = a$ gilt nämlich

$$a_{st} = b^{-1}st(b) = b^{-1}s(b)s(b^{-1}t(b)) = a_s s(a_t)$$

für alle $s,t \in G$. Ist $b' \in B$ so, daß $p(b') = p(b) = c$ gilt, dann existiert ein $a \in A$, so daß $b' = ba$. Sei $\alpha' : G \to A$, $\alpha'(s) := a'_s := i^{-1}(b'^{-1}s(b'))$, der 1-Kozykel, der mit Hilfe von b' definiert ist. Dann gilt $a'_s = a^{-1}b^{-1}s(b)s(a) =$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$a^{-1}a_s s(a)$ für alle $s \in G$. Also ist α' aequivalent zu α. Daher ist eine Abbildung $\delta : H^0(G,C) \to H^1(G,A)$ durch

$\delta(c) :=$ Aequivalenzklasse von α

wohldefiniert. Es gilt $\delta(1) = (\mathtt{1})$.
Wir machen nun die zusätzliche Annahme:

$A \leq$ Zentrum von B.

Dann ist die G-Gruppe A insbesondere kommutativ, und $H^2(G,A)$ ist definiert. Wir wollen in dieser Situation eine Abbildung

$\Delta : H^1(G,C) \to H^2(G,A)$,

ebenfalls Korandabbildung genannt, definieren. Sei dazu $\gamma : G \to C$, $\gamma(s) = c_s$, ein 1-Kozykel und sei $\beta : G \to B$, $\beta(s) = b_s$, eine Abbildung mit der Eigenschaft

$p(b_s) = c_s$ für alle $s \in G$.

Dann gilt

$a_{s,t} := b_s s(b_t) b_{st}^{-1} \in A$ für alle $s,t \in G$

$(p(b_{st}) = c_{st},\ p(b_s)p(s(b_t)) = c_s s(p(b_t)) = c_s s(c_t) = c_{st})$.

Wir zeigen, daß durch

$\alpha : G \times G \to A,\ \alpha((s,t)) := a_{s,t};\ s,t \in G,$

ein 2-Kozykel definiert ist: Die zu überprüfende Identität ist

$s(a_{t,u})a_{s,tu} = a_{st,u}a_{s,t}; \quad s,t,u \in G.$

Sie ist aequivalent zu

$a_{s,t}^{-1}a_{s,tu}a_{st,u}^{-1}s(a_{t,u}) = 1; \quad s,t,u \in G;$

oder zu

$$b_{st}s(b_t)^{-1}b_s^{-1}b_s s(b_{tu})b_{stu}^{-1}b_{stu}st(b_u)^{-1}b_{st}^{-1}s(a_{t,u}) \ = \quad .$$

$$= \quad b_{st}s(b_t)^{-1}s(b_{tu})st(b_u)^{-1}b_{st}^{-1}s(a_{t,u}) = 1; \quad s,t,u \in G$$

Für alle $s,t,u \in G$ ist

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$s(a_{t,u}) = s(b_t)st(b_u)s(b_{tu}^{-1}) \in$ Zentrum von B.

Also ist zu zeigen, daß

$b_{st}s(b_t)^{-1}s(b_t)st(b_u)s(b_{tu}^{-1})s(b_{tu})st(b_u)^{-1}b_{st}^{-1} = 1$

für alle $s, t, u \in G$. Das ist jedoch offensichtlich.

Sei nun $\gamma' : G \to C$, $\gamma'(s) := c'_s$, ein zu γ aequivalenter 1-Kozykel. Dann existiert ein $c \in C$ mit

$c'_s = c^{-1}c_s s(c)$ für alle $s \in G$.

Sei $b \in B$ ein Urbild von c unter p, also $p(b) = c$. Setze

$\beta'(s) := b'_s := b^{-1}b_s s(b)$, $s \in G$.

Es gilt

$\alpha'(s,t) := a'_{s,t} := b'_s s(b'_t)b'^{-1}_{st} =$

$= b^{-1}b_s s(b)s(b^{-1})s(b_t)st(b)st(b)^{-1}b_{st}^{-1}b =$

$= b^{-1}a_{s,t}b = a_{s,t}$

für alle $s, t \in G$; letzteres, weil A nach Annahme im Zentrum von B enthalten ist.

Ändert man b_s zu $b'_s := a_s b_s$ mit $a_s \in A$, dann gilt

$a'_{s,t} = a_s b_s s(a_t)b_t b_{st}^{-1}a_{st}^{-1} = a_s s(a_t)a_{st}^{-1}a_{s,t}$

für alle $s, t \in G$, weil $A \leq Zentrum(B)$. Also ist der 2-Kozykel

$\alpha' : G \times G \to A$, $\alpha'((s,t)) := a'_{s,t}$,

aequivalent zu dem 2-Kozykel

$\alpha : G \times G \to A$, $\alpha((s,t)) = a_{s,t}$.

Durch die Festsetzung

$\Delta((\gamma)) := (\alpha)$

ist damit eine Abbildung von Kohomologiemengen

$\Delta : H^1(G,C) \to H^2(G,A)$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

mit der Eigenschaft $\Delta((\mathtt{1})) = (1)$ wohldefiniert.

(4.6) **Satz** (Serre [$SE1$], Chapter VII, Appendix, Proposition 2) *Sei G eine Gruppe und sei*

$$1 \to A \xrightarrow{i} B \xrightarrow{p} C \to 1$$

eine exakte Sequenz von - nicht notwendigerweise kommutativen - G-Gruppen. Dann ist die folgende induzierte Sequenz von Abbildungen punktierter Kohomologiemengen exakt:

$$1 \to H^0(G,A) \xrightarrow{i_0} H^0(G,B) \xrightarrow{p_0} H^0(G,C) \xrightarrow{\delta}$$

$$\xrightarrow{\delta} H^1(G,A) \xrightarrow{i_1} H^1(G,B) \xrightarrow{p_1} H^1(G,C).$$

Wenn außerdem A im Zentrum von B enthalten ist, dann ist auch die folgende Sequenz von Abbildungen punktierter Kohomologiemengen exakt

$$1 \to H^0(G,A) \xrightarrow{i_0} H^0(G,B) \xrightarrow{p_0} H^0(G,C) \xrightarrow{\delta} H^1(G,A) \xrightarrow{i_1}$$

$$\xrightarrow{i_1} H^1(G,B) \xrightarrow{p_1} H^1(G,C) \xrightarrow{\Delta} H^2(G,A).$$

Beweis: (1) Die Exaktheit bei $H^0(G,A)$ ist offensichtlich.

(2) Zur Exaktheit bei $H^0(G,B)$: Es gilt $p_0 = i_0 = \mathtt{1}$, wobei $\mathtt{1}$ die konstante Abbildung bezeichnet, die jedes Element auf 1 abbildet. Ist umgekehrt $b \in B^G \cap Kern(p_0)$, dann ist $b \in A \cap B^G = i_0(A^G)$.

(3) Zur Exaktheit bei $H^0(G,C)$: Ein beliebiges Element $c \in C^G$ genhört genau dann zu $p_0(B^G)$, wenn ein $b \in B^G$ mit der Eigenschaft $p(b) = c$ existiert. Und $\delta(c) = 1$ bedeutet aufgrund der Definition von δ dasselbe (Für alle $s \in G$ ist $1 = a_s = b^{-1}s(b)$ für ein $b \in p^{-1}(c)$).

(4) Zur Exaktheit bei $H^1(G,A)$: Sei $\alpha \in Z^1(G,A)$, $\alpha(s) = a_s$, ein 1-Kozykel, dessen Klasse im Kern von i_1 liegt. Das bedeutet, daß ein $b \in B$ existiert, so daß $a_s = b^{-1}s(b)$ für alle $s \in G$. Die letztgenannte Bedingung ist sicherlich erfüllt, wenn $(\alpha) \in H^1(G,A)$ im Bild von δ enthalten ist. Ist umgekehrt (α) enthalten im Bild von δ, etwa $\alpha(s) = a_s = b^{-1}s(b)$ mit $b \in B$, dann ist $p(b) \in C^G$, und $p(b)$ ist gleich $\delta((\alpha))$.

(5) Zur Exaktheit bei $H^1(G,B)$: Es gilt $p_1 \circ i_1 = \mathtt{1}$. Sei umgekehrt $\beta : G \to B$ ein 1-Kozykel, so daß für alle $s \in G$ $p(\beta(s)) = p(b)^{-1}s(p(b))$ mit einem Element $b \in B$. Dann existiert ein 1-Kozykel $\alpha : G \to A$, $\alpha(s) = a_s$, so daß $\beta(s) = b^{-1}s(b)a_s$; d.h. $(\beta) \in H^1(G,B)$ ist im Bild von i_1 enthalten.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

(6) Zur Exaktheit bei $H^1(G, C)$ unter der Voraussetzung $A \leq Zentrum(B)$: Aus der Definition folgt $\Delta \circ p_1 = 1$.Sei umgekehrt $\gamma : G \to C$, $\gamma(s) = c_s$, ein 1-Kozykel, dessen Klasse im Kern von Δ liegt. Sei $\beta : G \to B$, $\beta(s) = b_s$, eine Abbildung mit $c_s = p(b_s)$ für alle $s \in G$. Dann ist der durch

$$\Delta(\gamma)((s,t)) = b_s s(b_t) b_{st}^{-1}, \quad s, t \in G,$$

gegebene 2-Kozykel $G \times G \to A$ aequivalent zum trivialen 2-Kozykel, d.h. es gibt eine Abbildung $G \to A$, $s \mapsto a_s$, so daß

$$\Delta(\gamma)((s,t)) = a_s s(a_t) a_{st}^{-1} \quad \text{für alle} \quad s, t \in G.$$

Ersetzt man b_s für alle s durch $a_s^{-1} b_s$, dann gilt $\Delta(\gamma)((s,t)) = 1$ für alle $s, t \in G$. Somit ist die Abbildung $G \to B$, $s \mapsto b_s$, ein 1-Kozykel mit der Eigenschaft $c_s = p(b_s)$ für alle $s \in G$.

Damit ist der Beweis von (4.6) beendet

(4.7) **Beispiele** (a) (Vgl. $[SCH]$) Sei K ein Körper und sei G eine Gruppe, die trivial auf den Gruppen in der folgenden exakten Sequenz operiert

$$1 \to K^* \to GL(n,K) \xrightarrow{p} PGL(n,K) \to 1.$$

Nach (4.6) ist die folgende Sequenz von Abbildungen punktierter Kohomologiemengen exakt

$$Hom(G, K^*) \to H^1(G, GL(n,K)) \to H^1(G, PGL(n,K)) \xrightarrow{\Delta = \Delta_n} H^2(G, K^*).$$

Die Menge $H^1(G, GL(n,K))$ bzw. $H^1(G, PGL(n,K))$ besteht aus den Aequivalenzklassen linearer bzw. projektiver Matrixdarstellungen von G vom Grad n über K. Die zu einer Aequivalenzklasse einer projektiven Darstellung $P : G \to PGL(n,K)$ gehörige Kozykelklasse $(\Delta(P))$ ist genau dann trivial, wenn sich P zu einer linearen Darstellung $D : G \to GL(n,K)$ liften läßt, d.h. wenn P über D faktorisiert:

$$P = p \circ D : G \xrightarrow{D} GL(n,K) \xrightarrow{p} PGL(n,K).$$

Außerdem folgt, daß jede Liftung von P aequivalent zu einer Liftung der Form $\lambda \otimes D$ ist, wobei D eine fest gewählte Liftung von P ist und $\lambda \in Hom(G, K^*)$. Die im Bild von Δ enthaltenen 2-Kozykelklassen $(\alpha) \in H^2(G, K^*)$ haben alle die Eigeschaft $(\alpha)^n = (1)$. Ist nämlich $(\alpha) = (\Delta(P))$ und ist $\rho : PGL(n,K) \to GL(n,K)$ ein Schnitt zu $p : GL(n,K) \to PGL(n,K)$, dann gilt für $T := \rho \circ P$:

$$T(s)T(t) = \alpha(s,t)T(st) \quad \text{für alle} \quad s, t \in G.$$

Nach einer auf I. Schur zurückgehenden Schlußweise, vgl. $[SCH]$, §1, Beweis von Satz I, folgt durch Bildung der Determinante aus dieser Gleichung

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$\alpha^n(s,t) = \det(T(s))\det(T(t))\det(T(st))$ für alle $s,t \in G$,

also $\alpha^n \sim 1$. Ist $n = |G|$, dann ist die Abbildung Δ_n surjektiv. Um das einzusehen betrachten wir die Gruppenalgebra

$V := K[G] := \bigoplus_{s\in G} Ke_s$

von G über K als $K-$Vektorraum und definieren, nach Identifikation von V mit K^n vermöge der $K-$Basis e_s, $s \in G$, zu vorgegebener 2-Kozykelklasse $(\alpha) \in H^2(G, K^*)$ eine Abbildung $T : G \to GL(n, K)$ durch

$T(s)(e_t) := \alpha(s,t)e_{st}$, $s,t \in G$.

Man rechnet nach, daß

$T(s)T(t) = \alpha(s,t)T(st)$ für alle $s,t \in G$

gilt, so daß also durch

$P(s) := p(T(s))$, $s \in G$,

ein Element $(P) \in H^1(G, PGL(n,K))$ mit der Eigenschaft $\Delta_n((P)) = (\alpha)$ definiert ist.

(b) Ist $G = G(K/k)$ die Galoisgruppe einer endlichen Galoiserweiterung K/k, dann ist

$1 \to K^* \to GL(n,K) \xrightarrow{p} PGL(n,K) \to 1$

eine exakte Sequenz von G-Gruppen. Wegen $H^1(G, GL(n,K)) = 1$, vgl. (1.8), hat man daher die folgende Abbildung von Kohomologiemengen mit trivialem Kern

$H^1(G, PGL(n,K)) \xrightarrow{\Delta=\Delta_n} H^2(G, K^*)$.

Man kann sogar zeigen, daß Δ im vorliegenden Fall injektiv ist.

Ähnlich wie im vorangehenden Beispiel (a) beweist man mit der Schurschen Determinantenmethode, daß alle (α), die im Bild von Δ_n liegen, die Eigenschaft $(\alpha)^n \sim (1)$ besitzen. Für $n = |G|$ ist Δ_n surjektiv, wie man mit einem ähnlichen Argument wie im Beispiel (a) beweist, vgl. z.B. [$SE1$], Chapter X, §5, proof of lemma 1: Man betrachtet wieder die Gruppenalgebra $V := (K,G) = \bigoplus_{s\in G} Ke_s$ als n-dimensionalen $K-$Vektorraum und definiert, nach Identifikation von V mit K^n vermöge der Basis e_s, $s \in G$, zu vorgegebenem $(\alpha) \in H^2(G, K^*)$ eine Abbildung $T : G \to GL(V)$ durch

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$T(s)(e_t) := \alpha(s,t)T(e_{st}), \ \ s,t \in G,$

und erhält damit das Element $(P) := (p \circ T) \in H^1(G, PGL(n,K))$ mit der Eigenschaft $\Delta_n((P)) = (\alpha)$.

Aufgaben und Beispiele

(1) Sei G eine freie Gruppe und sei A ein G-Modul. Beweisen Sie, daß die Gruppe $H^2(G,A)$ trivial ist. (Wohlbekannt; folgt sofort aus der universellen Eigenschaft der freien Gruppe)

(2) Sei C_2 eine zyklische Gruppe der Ordnung 2. Bestimmen Sie einen zentralen 2-Kozykel $f : C_2 \times C_2 \to C_2$, so daß die durch f bestimmte zentrale gruppenerweiterung von $C_2 \times C_2$ mit Kern C_2 isomorph zur Diedergruppe der Ordnung 8 ist. (Vgl. Bücher über Gruppentheorie)

(3) Beweisen Sie Satz (4.5), d.h. beweisen Sie die Exaktheit der dort aufgeführten Sequenz von Kohomologiegruppen. (Vgl. dazu auch $[H]$)

(4) Erarbeiten Sie anhand der Arbeit $[H]$ eine nichtkommutative Verallgemeinerung von Satz (4.5).

(5) Sei $\mathcal{G}$ eine Gruppe und sei G ein epimorphes Bild von $\mathcal{G}$ mit dem Epimorphismus $p : \mathcal{G} \to G$. Sei $1 \to A \to E \xrightarrow{q} G \to 1$ eine Gruppenerweiterung mit abelschem Kern A und mit dem zugehörigen 2-Kozykel $c : G \times G \to A$. Zeigen Sie, daß die folgenden Aussagen aequivalent sind:

(a) Es existiert ein Homomorphismus $\varphi : \mathcal{G} \to E$, so daß $q \circ \varphi = p$

(b) $(c) \in H^2(G,A)$ liegt im Kern des Inflationshomomorphismus
$\inf : H^2(G,A) \to H^2(\mathcal{G},A)$.

Ist (a) oder (b) erfüllt, dann sagt man, daß das durch die Gruppenerweiterung definierte *Einbettungsproblem* $E(G,A,c)$ *für* $\mathcal{G}$ *lösbar* ist.

(Man kann (4.5) anwenden; vgl. dazu auch $[HM]$, 1.2 und 2.1)

(6) Beweisen Sie für $r = 1$ und $r = 2$ das folgende Resultat von Sah: Sei G eine Gruppe und sei A ein G-Modul. Angenommen α ist ein nichttriviales Element im Zentrum von G. Dann werden die Kohomologiegruppen $H^r(G,A)$, $r \geq 1$, durch die Abbildung $H^r(G,A) \to H^r(G,A)$, die durch den G-Homomorphismus $\widetilde{\alpha} : A \to A$, $x \mapsto \alpha(x) - x$, definiert wird, annulliert. Ist insbesondere $\widetilde{\alpha}$ ein Automorphismus von A, dann ist $H^r(G,A) = 0$. (Vgl. $[SAH]$ oder $[LG3]$, p.118/119)

(7) Beweisen Sie das folgende Resultat von H. Hasse: Sei k ein Zahlkörper, sei μ_m die Gruppe aller Einheitswurzeln in einem algebraischen Abschluß von k und sei $k' := k(\mu_m)$. Zeigen Sie: Ist m Potenz einer ungeraden Primzahl oder ist m eine Potenz von 2 und $\mu_4 \subset k$, dann ist $H^1(G(k'/k), \mu_m) = 1$; dabei wird μ_m als $G(k'/k)$-Modul bezüglich der Galoisoperation aufgefaßt. (Vgl. Aufgabe 6 oder $[NK]$, (4.8))

(8) Sei p eine Primzahl $\neq 2$. Zeigen Sie, daß bezüglich der natürlichen Operation von $GL(2,\mathbb{F}_p)$ auf dem 2-dimensionalen $\mathbb{F}_p$-Vektorraum $\mathbb{F}_p \times \mathbb{F}_p$ die Gruppe $H^1(GL(2,\mathbb{F}_p), \mathbb{F}_p \times \mathbb{F}_p)$ trivial ist. (Vgl. Aufgabe 6)

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

(9) Sei G eine endliche zyklische Gruppe der Ordnung n, sei s ein erzeugendes Element von G und sei A ein multiplikativ geschriebener G-Modul. Für $a \in A^G$

sei $f_a : G \times G \to A$ die wie folgt definierte Abbildung:

$$f_a(s^i, s^j) := \begin{cases} 1, \text{ falls } i+j < n \\ a, \text{ falls } i+j \geq n \end{cases}$$

Außerdem sei

$$N_G A := \left\{ \prod_{i=0}^{n-1} s^i(a) : a \in A \right\}$$

Zeigen Sie:
(a) f_a ist ein 2-Kozykel
(b) Die Abbildung

$$A^G / N_G A \to H^2(G, A), \;\; a \bmod N_G A \mapsto (f_a)$$

ist ein Isomorphismus. (Vgl. Bücher über Kohomologie von Gruppen)

(10) Sei G eine Gruppe und sei
$1 \to A \xrightarrow{i} B \xrightarrow{p} C \to 1$

eine exakte Sequenz von Links-G-Gruppen, so daß $i(A)$ im Zentrum von B enthalten ist. Wir wollen eine gruppentheoretische Interpretation der Elemente in $H^1(G, C)$ geben und folgen dabei der entsprechenden Darstellung in § 2 der Arbeit [RQ] von P. Roquette. Sei dazu

$$\bar{B} := \{(b, s) : b \in B, s \in G\},$$

versehen mit der Multiplikation

$$(b, s)(b', t) := (bb'^s, st);$$

$\bar{B}$ ist also das semidirekte Produkt von B mit G bezüglich der gegebenen Operation von G auf B. Insbesondere gilt

$$B \cap G = 1, \; B \cdot G = \bar{B},$$

wobei $B \cdot G$ die von B und G erzeugte Untergruppe in $\bar{B}$ bezeichnet. Sei $U \leq \bar{B}$ eine Untergruppe mit den folgenden Eigenschaften:

$$(\#) \quad B \cap U = A, \;\; B \cdot U = \bar{B};$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

d.h. U ist eine Gruppenerweiterung von $U/A = U/(B \cap U) \cong B \cdot U/B = \overline{B}/B \cong G$ mit dem Kern A, so daß also eine exakte Sequenz der folgenden Form besteht:

$$1 \to A \to U \xrightarrow{\pi} G \to 1$$

Sei $u : G \to U$, $s \mapsto u_s$, ein Schnitt zu π. Es gilt

$$u_s = b_s s$$

mit einem Element $b_s \in B$. Das Element $p(b_s) \in C$ ist durch s eindeutig bestimmt. Aus $\pi(u_s u_t) = \pi(u_{st})$ folgt

$$p(b_s)p(b_t)^s = p(b_{st}) \quad \text{für alle } s, t \in G.$$

Somit ist

$$\beta : G \to C,\ \beta(s) := p(b_s),$$

ein 1-Kozykel, der durch die Gruppenerweiterung U von G mit dem Kern A eindeutig bestimmt ist. Außerdem läßt sich jedes Element aus U in eindeutiger Weise in der Form $au_s = ab_s s$ mit $a \in A$, $s \in G$, $b_s \in B$ darstellen. Ist umgekehrt $\beta : G \to C$, $\beta(s) = c_s$, ein 1-Kozykel und sind $b_s \in B$ so, daß $p(b_s) = c_s$ für alle $s \in G$, dann bildet

$$U := \{(ab_s, s) : a \in A, s \in G\} \leq \overline{B}$$

eine Untergruppe von $\bar{B}$ mit den Eigenschaften (#).

Wir zeigen nun, daß je zwei Untergruppen U, U' von $\bar{B}$ mit den Eigenschaften (#) genau dann B-konjugiert sind, wenn die zugehörigen 1-Kozykeln $\beta, \beta' : G \to C$ aequivalent sind. Dabei benutzen wir die Relation

$$b^{-1}(b_s s)b = b^{-1} b_s b^{s^{-1}} s,\ b \in B,\ s \in G.$$

Sie zeigt, daß für beliebiges $b \in B$

$$U' = b^{-1} U b$$

genau dann gilt, wenn

$$\beta'(s) = p(b)^{-1}\beta(s)p(b)^s \quad \text{für alle} \quad s \in G$$

erfüllt ist; also genau dann, wenn die 1-Kozykeln β, β' vermöge $p(b)$ aequivalent sind. Somit ist bewiesen, vgl. [RQ], § 2,

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Satz *Die B-Konjugationsklassen von Untergruppen $U \leq \bar{B}$ mit den Eigenschaften (#) entsprechen unter der beschriebenen Korrespondenz bijektiv den Elementen von $H^1(G, C)$.*

§ 5. Projektive und induktive Grenzwerte

In diesem Abschnitt werden grundlegende Eigenschaften von projektiven und induktiven Grenzwerten zusammengestellt, die für die Galoiskohomologie von Bedeutung sind. Dabei folgen wir entsprechenden Ausführungen in $[KC]$, §1; in $[KP]$, Chapter 3, §1 sowie in $[H1]$, 2.4.1 und 2.4.2. Außerdem stellen wir Hilfsmittel aus der mengentheoretischen Topologie zusammen, die in vielen einschlägigen Lehrbüchern, z.B. in $[FR]$ oder $[J]$, zu finden sind; vgl. dazu auch $[H1]$, 2.4.1.

Zunächst definieren wir projektive und induktive Systeme. Dazu gehen wir aus von einer geordneten Menge $(I, \leq)$, d.h. I ist eine nichtleere Menge und $\leq$ ist eine reflexive, transitive und antisymmetrische Relation, eine sogenannte Ordnungsrelation. Eine geordnete Menge $(I, \leq)$ heißt *gerichtet*, wenn für alle $i, j \in I$ ein $k \in I$ existiert, so daß $i \leq k$ und $j \leq k$.

Definition Sei $(I, \leq)$ eine geordnete und gerichtete Menge und sei $\mathfrak{A}$ eine Kategorie. Ein *projektives* oder *inverses* bzw. *induktives System von $\mathfrak{A}$ über I* ist eine Familie

$$(I, X_i, f_{ij})_{i,j \in I. i \leq j}$$

mit Objekten X_i von $\mathfrak{A}$ und Morphismen

$$f_{ij} : X_j \to X_i \quad \text{bzw.} \quad f_{ij} : X_i \to X_j$$

von $\mathfrak{A}$ für alle $i \in I$ und alle $i, j \in I$ mit $i \leq j$, so daß gilt

(a) $f_{ii} = id_{X_i}$ für alle $i \in I$

(b) $f_{ik} = f_{ij} \circ f_{jk}$ bzw. $f_{ik} = f_{jk} \circ f_{ij}$
für alle $i, j, k \in I$ mit $i \leq j \leq k$

(5.1) **Beispiele** (a) Sei p eine Primzahl, sei $I = \mathbb{N}$, versehen mit der natürlichen Ordnung $\leq$; sei $\mathfrak{A}$ die Kategorie der kommutativen Ringe, und für $i, j \in I$ mit $i \leq j$ sei $f_{ij} : \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$, der Homomorphismus von Restklassenringen, der jeder Restklasse $x + p^j\mathbb{Z}$ die entsprechende Restklasse $x + p^i\mathbb{Z}$ zuordnet. Dann ist $(I; \mathbb{Z}/p^i\mathbb{Z}, f_{ij})$ ein projektives System von $\mathfrak{A}$ über I.

(b) Sei p eine Primzahl, sei $I = \mathbb{N}$, versehen mit der natürlichen Ordnung $\leq$; sei $\mathfrak{A}$ die Kategorie der kommutativen Gruppen. Für jedes $i \in I$ sei $(\mathbb{Z}/p^i\mathbb{Z})^*$ die Einheitengruppe des Restklassenringes $\mathbb{Z}/p^i\mathbb{Z}$ und für $i, j \in I$ mit $i \leq j$ sei $f_{ij} : (\mathbb{Z}/p^j\mathbb{Z})^* \to (\mathbb{Z}/p^i\mathbb{Z})^*$ der Homomorphismus von Gruppen, der $x +$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$p^j\mathbb{Z} \in (\mathbb{Z}/p^j\mathbb{Z})^*$ auf $x + p^i\mathbb{Z} \in (\mathbb{Z}/p^i\mathbb{Z})^*$ abbildet. Dann ist $(I, (\mathbb{Z}/p^i\mathbb{Z})^*, f_{ij})$ ein projektives System von $\mathfrak{A}$ über I.

(c) Sei $I = \mathbb{N}$, versehen mit der Teilbarkeitsrelation / ; sei $\mathfrak{A}$ die Kategorie der kommutativen Gruppen, und für jedes $m \in \mathbb{N}$ sei μ_m die Gruppe der m-ten Einheitswurzeln in $\mathbb{C}$. Für $m, n \in \mathbb{N}$ mit m/n sei $f_{m,n} : \mu_m \to \mu_n$ die Einbettung $\mu_m \hookrightarrow \mu_n$. Dann ist $(I, \mu_m, f_{m,n})$ ein induktives System von $\mathfrak{A}$ über I.

(d) Sei k ein Körper und sei $\mathfrak{F}$ eine k-Kategorie über einer Kategorie $\mathfrak{G}(k)$ von Körpererweiterungen von k, die alle in einem gemeinsamen Oberkörper enthalten sind. Sei K/k eine Körpererweiterung in $\mathfrak{G}(k)$. Sei $\{K_i/K : i \in I\}$ die Menge aller Körpererweiterungen von K in $\mathfrak{G}(k)$. Für $i, j \in I$ sei $i \leq j$, falls K_i Teilkörper von K_j ist. Durch diese Festsetzung wird I zu einer gerichteten Menge, wobei eine obere Schranke für K_i/k und K_j/k durch das Kompositum von K_i und K_j in dem zugrundegelegten gemeinsamen Oberkörper gegeben ist. Sei X ein K-Objekt von $\mathfrak{F}$ und sei $E_{\mathfrak{F}}(K_i/K, X)$ die Menge aller K-Isomorphieklassen von K_i/K-Twistungen von X. Für $i \leq j$ sei

$$f_{jl} : E_{\mathfrak{F}}(K_i/K, X) \to E_{\mathfrak{F}}(K_j/K, X)$$

die Abbildung, die jeder K_i/K-Twistung von X die entsprechende K_j/K-Twistung von X zuordnet. Dann ist

$$(I, E_{\mathfrak{F}}(K_i/K, X), f_{ij})$$

ein induktives System von der Kategorie der Mengen mit ausgezeichnetem Element über I.

Nun definieren wir projektive und induktive Grenzwerte.

Definition Sei $(I, \leq)$ eine geordnete und gerichtete Menge und sei $\mathfrak{A}$ eine Kategorie. Sei (I, X_i, f_{ij}) ein projektives System von $\mathfrak{A}$ über I, so daß das Produkt $\prod_{i\in I} X_i$ in $\mathfrak{A}$ definiert ist (vgl. §1). Der *projektive* oder *inverse Grenzwert* (Limes) dieses projektiven Systems ist, falls es existiert, ein Objekt X von $\mathfrak{A}$, das sich in der folgenden Form darstellen läßt:

$$X := \varprojlim{}_{i\in I} X_i :=$$

$$:= \{x \in \textstyle\prod_{i\in I} X_i : f_{ij}(p_j(x)) = p_i(x) \quad \text{für alle} \;\; i, j \in I \;\; \text{mit} \;\; i \leq j\};$$

dabei bezeichnen die $p_i : \prod_{i\in I} X_i \to X_i$ die Projektionsabbildungen.

Sei (I, X_i, f_{ij}) ein induktives System von $\mathfrak{A}$ über I, so daß das Koprodukt $\coprod_{i\in I} X_i$ in $\mathfrak{A}$ definiert ist (vgl. § 1). Der *induktive Grenzwert (Limes)* dieses induktiven Systems ist, falls es existiert, ein Objekt X von $\mathfrak{A}$, das sich in der folgenden Form darstellen läßt

$$X := \varinjlim{}_{i\in I} X_i := \cup_{i\in I} f_i(X_i)/ \sim,$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

wobei $f_i : X_i \to \coprod_{i\in I} X_i$ jeweils die Inklusion und $\cup_{i\in I} f_i(X_i)/\sim$ die Quotientenmenge bezüglich der wie folgt definierten Aequivalenzrelation $\sim$ bezeichnet.: $x = f_i(x_i) \in f_i(X_i)$ heißt aequivalent zu $y = f_j(x_j) \in f_j(X_j)$, falls ein $k \in I$ mit $i \leq k$, $j \leq k$ und $f_{ik}(x_i) = f_{jk}(x_j)$ existiert.

Wenn ein projektiver bzw. induktiver Grenzwert existiert, so ist er aufgrund seiner Konstruktion eindeutig bestimmt. Verschiedene projektive bzw. induktive Systeme können denselben Grenzwert haben.

(5.2) **Beispiele** (a) Für das in (5.1), (a), gegebene projektive System heißt dessen projektiver Grenzwert

$$\mathbb{Z}_p := \varprojlim_{i\in\mathbb{N}} \mathbb{Z}/p^i\mathbb{Z}$$

der Ring der p-adischen ganzen Zahlen. Er ist nullteilerfrei und sein Quotientenkörper $\mathbb{Q}_p$ heißt der Körper der rationalen p-adischen Zahlen.

(b) Für das in (5.1), (b), gegebene projektive System ist dessen projektiver Grenzwert die Einheitengruppe $\mathbb{Z}_p^*$ des Ringes $\mathbb{Z}_p$.

(c) Der induktive Grenzwert des in (5.1), (c), gegebenen induktiven Systems ist die Gruppe aller Einheitswurzeln in $\mathbb{C}$.

(d) Sei G eine Gruppe oder ein kommutativer Ring. Sei

$$\mathcal{N} := \{N_i : i \in I\}$$

eine Menge von normalen Untergruppen bzw. Idealen von G, die in G endlichen Index haben. Wir nehmen an, daß $\mathcal{N}$ bezüglich der Bildung endlich vieler Durchschnitte abgeschlossen ist. Die Indexmenge I wird durch die folgende Festsetzung zu einer geordneten Menge: Für $i, j \in I$ sei $i \leq j$ genau dann, wenn $N_i \supset N_j$ gilt. Dann ist I eine gerichtete Menge, weil mit N_i und N_j auch der Normalteiler $N_k := N_i \cap N_j$ von G - als Kern des Homomorphismus $G \to G/N_i \times G/N_j$, $g \mapsto (gN_i, gN_j)$ - endlichen Index besitzt. Außerdem sei für $i, j \in I$ mit $i \leq j$ die Abbildung

$$f_{i,j} : G/N_j \to G/N_i$$

die durch $N_j \subset N_i$ induzierte Projektionsabbildung. Dann ist $(I, G/N_i, f_{i,j})$ ein projektives System. Sei $G^{\mathcal{N}}$ dessen projektiver Grenzwert. Ist $\mathcal{N}$ die Menge aller normalen Untergruppen bzw. Ideale von G von endlichem Index, dann heißt $G^{\mathcal{N}}$ die totale Vervollständigung von G. Ist p eine Primzahl und $\mathcal{N}$ die Menge aller normalen Untergruppen bzw. Ideale von G mit p-Potenz Index, dann heißt $G^{\mathcal{N}}$ die p-Vervollständigung von G. Beispielsweise ist die p-Vervollständigung des Ringes $\mathbb{Z}$ isomorph zum Ring $\mathbb{Z}_p$ aller p-adischen ganzen Zahlen (vgl. (a)). Die totale Vervollständigung von $\mathbb{Z}$ ist aufgrund des chinesischen Restsatzes isomorph zum direkten Produkt der Ringe $\mathbb{Z}_p$, p Primzahl.

(e) Sei k ein Körper, sei $\overline{k}$ ein separabler algebraischer Abschluß von k, sei $\mathfrak{G}(k)$ die Kategorie aller Körpererweiterungen von k in $\overline{k}$ und sei $\mathfrak{F}$ eine

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

k-Kategorie über $\mathfrak{G}(k)$. In dem in Beispiel (5.1), (d), genannten induktiven System betrachten wir für eine beliebige Körpererweiterung K/k in $\overline{k}$ und ein beliebiges K-Objekt X von $\mathfrak{F}$ das Teilsystem $(I_0, E_{\mathfrak{F}}(K_i/K, X), f_{ij})$, bei dem K_i/K, $i \in I_0$, alle Erweiterungen in $\overline{k}$ mit endlichem Grad $(K_i : K)$ durchläuft und definieren

$$\overline{E}_{\mathfrak{F}}(K, X) := \varinjlim(I_0, E_{\mathfrak{F}}(K_i/K, X)).$$

Definition Eine Zwischenkörpererweiterung L/K von $\overline{k}/K$ heißt *Zerfällungskörper von* $(Y) \in E_{\mathfrak{F}}(\overline{k}/K, X)$, falls $(Y_L) \in E_{\mathfrak{F}}(\overline{k}/L, X_L)$ das triviale Element ist, d.h. falls ein L-Isomorphismus $Y_L \cong X_L$ existiert.

Bemerkung Wenn jedes Element aus $E_{\mathfrak{F}}(\overline{k}/K, X)$ einen Zerfällungskörper L mit endlichem Grad $(L : K)$ besitzt, dann ist $\overline{E}_{\mathfrak{F}}(K, X) = E_{\mathfrak{F}}(\overline{k}/K, X)$

Definition Wir nennen jedes K-Objekt X von $\mathfrak{F}$ mit der Eigenschaft, daß jedes Element aus $E_{\mathfrak{F}}(\overline{k}/K, X)$ einen Zerfällungskörper L mit endlichem Grad $(L : K)$ besitzt, ein *proendliches K-Objekt von $\mathfrak{F}$*.

(b) Für die folgenden Kategorien $\mathfrak{F}$ und K-Objekte X von $\mathfrak{F}$ besitzt jedes Element aus $E_{\mathfrak{F}}(\overline{k}/K, X)$ einen galoisschen Zerfällungskörper endlichen Grades:
(i) $\mathfrak{F}$ = k-Kategorie aller quadratischen Räume, X = nichtausgearteter quadratischer Raum über K (vgl. [SR], 2, Lemma 2.1)
(ii) $\mathfrak{F} = \mathfrak{T}_{1,2}$ = k-Kategorie aller Algebren, X = zentraleinfache K-Algebra (vgl. [D], Kapitel IV, §4, Satz 18)

Nachfolgend werden einige Grundbegriffe aus der Topologie zusammengestellt, die für die Untersuchung projektiver und induktiver Grenzwerte nützlich sind, vgl. z.B. [FR], [J].

Man sagt, daß auf einer Menge X eine *Topologie* gegeben ist, wenn für jedes $p \in X$ eine Menge von Teilmengen $\mathcal{U}(p)$ mit den folgenden Eigenschaften existiert:

Für alle $U \in \mathcal{U}(p)$ ist $p \in U$.
Wenn $U \in \mathcal{U}(p)$ und $V \supset U$, dann gilt $V \in \mathcal{U}(p)$.
Wenn $U_1, U_2 \in \mathcal{U}(p)$, dann ist $U_1 \cap U_2 \in \mathcal{U}(p)$.
Es ist $X \in \mathcal{U}(p)$.
Zu jedem $U \in \mathcal{U}(p)$ gibt es ein $V \in \mathcal{U}(p)$ so, daß $U \in \mathcal{U}(y)$ für alle $y \in V$.

Die Elemente aus $\mathcal{U}(p)$ nennt man *Umgebungen* von p, und die Familie

$$\mathcal{U} = (\mathcal{U}\ (p))_{p \in X}$$

heißt *Topologie auf X*. Jede Menge X zusammen mit einer Topologie $\mathcal{U}$ auf X heißt *topologischer Raum*.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Beispiel Die *diskrete Topologie* auf einer Menge X ist gegeben durch $\mathcal{U}(p) = \{\{p\} : p \in X\}$.

Sei $A \subset X$ eine Teilmenge eines topologischen Raumes $X = (X, (\mathcal{U}(p))_{p\in X})$. $p \in X$ heißt *innerer Punkt* von A, wenn ein $U \in \mathcal{U}(p)$ existiert, so daß $U \subset A$. $\overset{\circ}{A}$ sei die Menge aller inneren Punkte.von A. $p \in X$ heißt *äußerer Punkt* von A, wenn es ein $U \in \mathcal{U}(p)$ gibt, so daß $U \subset X \setminus A$. $p \in X$ heißt *Randpunkt* von A, wenn in jedem $U \in \mathcal{U}(p)$ Punkte von A und $X \setminus A$ liegen. ∂A sei die Menge aller Randpunkte von A. $p \in X$ heißt *Berührpunkt* von A, wenn in jeder Umgebung von p Punkte von A liegen. $\bar{A}$ sei die Menge aller Berührpunkte von A. A heißt *offen*, wenn A nur aus inneren Punkten besteht. A heißt *abgeschlossen*, wenn $A = \bar{A}$ gilt. $\overset{\circ}{A}$ ist offen und $\bar{A}$ ist abgeschlossen. A ist offen genau dann, wenn $X \setminus A$ abgeschlossen ist. $p \in X$ heißt *Häufungspunkt* von A, wenn p Berührpunkt von $A \setminus \{p\}$ ist $p \in X$ heißt *isolierter Punkt* von A, wenn es eine Umgebung von p gibt, in der p der einzige Punkt aus A ist. U ist Umgebung von $p \in X$ genau dann, wenn es eine offene Menge O gibt, so daß $p \in O \subset U$. Die Menge $\mathfrak{T}$ aller offenen Teilmengen eines topologischen Raumes X hat die folgenden Eigenschaften:

Die leere Menge $\emptyset$ und X gehören zu $\mathfrak{T}$.
Die Vereinigung beliebig vieler Elemente aus $\mathfrak{T}$ gehört zu $\mathfrak{T}$.
Der Durchschnitt endlich vieler Elemente von $\mathfrak{T}$ gehört zu $\mathfrak{T}$.

Ist umgekehrt $\mathfrak{T}$ eine Menge von Teilmengen einer Menge X, die diese Eigenschaften hat und nennt man eine Teilmenge $U \subset X$ Umgebung von $p \in X$, wenn es ein $O \in \mathfrak{T}$ mit $p \in O \subset U$ gibt, dann erhält man auf diese Weise zu jedem $p \in X$ eine Menge von Teilmengen $\mathcal{U}(p)$ von X, so daß $(X, (\mathcal{U}(p))_{p\in X})$ ein topologischer Raum ist.

Seien X, Y topologische Räume. Eine Abbildung $f : X \to Y$ heißt *stetig in* $x \in X$, wenn es für jede Umgebung V von $f(x)$ eine Umgebung U von x gibt, so daß $f(U) \subset V$. Somit ist $f : X \to Y$ *stetig*, d.h. stetig in jedem Punkt, wenn das Urbild jeder offenen Menge aus Y offen in X ist. Eine stetige Abbildung $f : X \to Y$ heißt *Homöomorphismus*, wenn f bijektiv ist und die Umkehrabbildung von f stetig ist.. Ein topologischer Raum X heißt *zusammenhängend*, wenn es keine Aufteilung von X in nichtleere offene Teilmengen gibt, d.h. wenn es keine Teilmengen $U, V \subset X$ gibt, die offen und nicht leer sind und für die $X = U \cup V$, $U \cap V = \emptyset$ gilt. Nennt man Punkte x, y eines topologischen Raumes X aequivalent, wenn x und y in einer zusammenhängenden Teilmenge von X enthalten sind, dann erhält man dadurch eine Aequivalenzrelation auf X. Die entsprechenden Aequivalenzklassen heißen *Zusammenhangskomponenten* von X; es sind abgeschlossene Teilmengen. X heißt *total unzusammenhängend*, wenn die Zusammenhangskomponenten jeweils nur aus einem Punkt bestehen. Sind X_1, X_2 topologische Räume, so heißt die in der Produktmenge $X := X_1 \times X_2$ definierte Topologie, deren offene Mengen von der Form $O_1 \times O_2$ mit offenen Mengen O_1 von X_1 und O_2 von X_2 sind, die

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Produkttopologie auf X. Sei X ein topologischer Raum, sei Y eine Menge und sei $f : X \to Y$ eine surjektive Abbildung. Die *Quotiententopologie* auf Y hat als offene Mengen diejenigen Teilmengen $V \subset Y$, deren Urbilder $f^{-1}(V)$ offene Teilmengen von X sind. Ist Y eine Teilmenge eines topologischen Raumes X, dann nennt man $V \subset Y$ offen, falls eine offene Teilmenge $O \subset X$ existiert, so daß $V = O \cap Y$. Durch diese Festsetzung erhält man eine Topologie auf Y, die sogenannte durch die Topologie von X auf Y induzierte *Spurtopologie.* Eine Menge $\mathfrak{B}$ von offenen Teilmengen eines topologischen Raums X heißt *Basis von* X, wenn jede offene Menge von X Vereinigung von Elementen aus $\mathfrak{B}$ ist. $\mathfrak{B}$ ist Basis von X genau dann, wenn zu jeder offenen Menge $O \subset X$ und zu jedem Punkt $p \in X$ ein $B \in \mathfrak{B}$ mit $p \in B \subset O$ existiert. Eine *Umgebungsbasis* eines Punktes p eines topologischen Raumes X ist eine Menge $\mathcal{U}'$ von Umgebungen von p, so daß jede Umgebung von p eine Menge aus $\mathcal{U}'$ enthält. Diejenigen Mengen B einer Basis von X, die einen festen Punkt p enthalten, bilden eine Basis $\mathfrak{B}(p)$ von offenen Umgebungen von p. Ist für jeden Punkt $p \in X$ die Menge von Teilmengen $\mathfrak{B}(p)$ eine Basis von offenen Umgebungen von p, dann ist $\mathfrak{B} := \cup_{p \in X}\mathfrak{B}(p)$ eine Basis von X. Ein topologischer Raum X heißt *kompakt*, wenn X *hausdorffsch* ist, d.h. je zwei verschiedene Punkte von X haben disjunkte offene Umgebungen, und wenn jede *Überdeckung* von X mit offenen Mengen, d.h. jede Darstellung von X als Vereinigung offener Teilmengen O_ν, eine endliche Teilüberdeckung enthält, d.h. Vereinigung von endlich vielen der offenen Mengen O_ν ist. Stetige Bilder kompakter Mengen sind kompakt und stetige Bilder zusammenhängender Mengen sind zusammenhängend. Man sagt, daß eine Teilmenge A eines topologischen Raumes X *dicht* in X liegt, wenn in jeder Umgebung eines jeden Punktes von X ein Punkt aus A liegt.

Die topologischen Räume - als Objekte - bilden zusammen mit den stetigen Abbildungen zwischen ihnen - als Morphismen - eine Kategorie $\mathfrak{Top}$

Die folgenden einfachen topologischen Aussagen werden in Lehrbüchern über Topologie bewiesen, vgl. z.B. [FR], [J].

(5.3) **Satz** *Für beliebige topologische Räume X, Y gelten die folgenden Aussagen*

(i) *Ist X hausdorffsch, dann ist jede kompakte Teilmenge $A \subset X$ abgeschlossen*

(ii) *Ist X diskret, dann ist X hausdorffsch*

(iii) *Ist X endlich, dann ist X genau dann hausdorffsch, wenn X diskret ist.*

(iv) *Ist $A \subset X$ eine dichte Teilmenge, dann ist $\bar{A} = X$*

(v) *Ist $f : X \to Y$ eine stetige Abbildung, dann gilt*

(a) *Wenn $A \subset X$ eine kompakte Teilmenge ist, dann ist $f(A)$ kompakt*

(b) *Wenn f injektiv ist, dann ist f ein Homöomorphismus, wenn Bilder $f(A)$ abgeschlossener Teilmengen $A \subset X$ abgeschlossen in Y sind.*

Sei $(X_i)_{i \in I}$ eine Familie von topologischen Räumen und sei $X := \times_{i \in I} X_i$ das cartesische Produkt der X_i. X wird mit der folgenden Festsetzung zu

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

einem topologischen Raum, dem sogenannten *topologischen Produktraum* der X_i, $i \in I$: Eine Basis für die Topologie auf X sind die Teilmengen der Form

$$\prod_{i\in S} U_i \times \prod_{i\in I\setminus S} X_i,$$

wobei $S \subset I$ eine endliche Teilmenge ist und U_i für $i \in S$ eine offene Teilmenge von X_i ist. Die Projektionsabbildungen

$$p_k : X \to X_k,\ (x_i)_{i\in I} \mapsto x_k,$$

sind dann stetig, weil für jede offene Teilmenge $U \subset X_k$ das Urbild

$$p_k^{-1}(U) = \{(x_i)_{i\in I} : x_i \in X_i \ \text{ für } \ i \neq j, x_j \in U\}$$

offen in X ist. Ist $Y \subset X$ eine Teilmenge des cartesischen Produkts $X = \times_{i\in I} X_i$ der X_i, dann werden die Restriktionen $p_{|X_k} : Y \to X_k$ ebenfalls als Projektionen bezeichnet; sie sind bezüglich der von der Produkttopologie von X auf Y induzierten Spurtopologie stetig. Ist die Topologie auf X_i jeweils diskret, dann bilden die folgenden Mengen eine Umgebungsbasis für die Topologie auf X :

$$\{x_k\} \times \prod_{i\in I\setminus\{k\}} X_i\ ,\ k \in I.$$

(5.4) **Satz** *In der Kategorie der topologischen Räume existieren stets Produkte.*

Beweis: Sei $(X_i)_{i\in I}$ eine Familie von topologischen Räumen, sei X das cartesische Produkt der X_i, versehen mit der oben definierten Produkttopologie, und seien $p_i : X \to X_i$ die zugehörigen Projektionsabbildungen. Sei Y ein weiterer topologischer Raum und seien $g_i : Y \to X_i$, $i \in I$, stetige Abbildungen. Dann ist die Abbildung

$$h : Y \to X,\ \ y \mapsto (g_i(y))_{i\in I}$$

stetig, weil die g_i stetig sind, und es gilt

$$p_i \circ h = g_i \ \text{ für alle } \ i \in I.$$

Ist $h' : Y \to X$ eine weitere stetige Abbildung mit der Eigenschaft $p_i \circ h' = g_i$ für alle $i \in I$, dann ist $h'(y) = ((g_i(y))_{i\in I}$ für alle $y \in Y$, d.h. es gilt $h = h'$. Damit ist der Beweis von (5.4) beendet.

.

(5.5) **Satz** *Sei (I, X_i, f_{ij}) ein projektives System von topologischen Räumen mit stetigen Abbildungen $f_{ij} : X_j \to X_i$. Dann existiert der projektive Grenzwert X dieses projektiven Systems, und es gilt:*

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

(i) Sind die X_i hausdorffsch, so auch X, und X ist abgeschlossen im topologischen Produktraum $\prod_{i\in I} X_i$.

(ii) Sind die X_i hausdorffsch und kompakt, dann ist auch X kompakt.

(iii) Sind die X_i total unzusammenhängend, dann ist auch X total unzusammenhängend.

Beweis: (i): Nach (5.4) existiert der topologische Produktraum $\prod_{i\in I} X_i$. Somit ist der projektive Grenzwert $X := \varprojlim X_i$ ein topologischer Raum bezüglich der auf X induzierten Spurtopologie. Sind die X_i hausdorffsch und sind $x = (x_i)$, $y = (y_i)$ zwei verschiedene Elemente aus X, dann gibt es ein $k \in I$, so daß $x_k \neq y_k$, d.h. $p_k(x) \neq p_k(y)$. Da X_k hausdorffsch ist, gibt es in X_k offene Umgebungen U_k von x_k sowie V_k von y_k mit der Eigenschaft $U_k \cap V_k = \emptyset$. Dann sind die Urbilder von U_k und V_k unter der stetigen Projektionsabbildung p_k offene Umgebungen von x bzw. y. Diese Urbilder sind disjunkt. Also ist X hausdorffsch. Für $j \leq k$ setze

$$X_{jk} := \{(x_i) \in \textstyle\prod_{i\in I} X_i : f_{jk}(x_k) = x_j\}$$

$$= \{x \in \textstyle\prod_{i\in I} X_i : (f_{jk} \circ p_k)(x) = p_j(x)\}.$$

Dann ist

$$X = \cap_{j,k\in I,\ j\leq k} X_{jk}.$$

Die X_{jk} sind abgeschlossen bezüglich der Produkttopologie auf $\prod_{i\in I} X_i$: Die Abbildungen p_j und $f_{jk} \circ p_k$ sind stetige Abbildungen von X nach X_j. Sei $Z := X_j \times X_j$. Dann ist die Abbildung

$$h : X \to Z,\ x \mapsto (p_j(x), (f_{jk} \circ p_k)(x)),$$

stetig. Die Teilmenge

$$Y := \{(x_j, y_j) \in Z : x_j = y_j\}$$

von Z ist abgeschlossen: Sei dazu $(x_j, y_j) \in Z \setminus Y$, d.h. $x_j \neq y_j$. Da X_j hausdorffsch ist, gibt es offene Umgebungen U von x_j und V von y_j mit der Eigenschaft $U \cap V = \emptyset$. Dann ist $U \times V$ eine offene Umgebung von (x_j, y_j) in Z, die kein Element von Y enthält. Also ist $Z \setminus Y$ offen und daher Y abgeschlossen. Da das Urbild von Y unter h gleich X_{jk} ist und da h stetig ist, ist X_{jk} abgeschlossen in X. Es folgt, daß X als Durchschnitt der abgeschlossenen Mengen X_{jk} abgeschlossen ist. Damit ist die Behauptung (i) bewiesen.

(ii): Sind die X_i außerdem kompakt, so ist nach einem bekannten Satz von Tychonoff der topologische Produktraum $\prod_{i\in I} X_i$ kompakt, vgl. z.B. [J], und daher X als abgeschlossene Teilmenge eines kompakten und nach (i) auch hausdorffschen topologischen Raumes ebenfalls kompakt.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

(iii): Da die Projektionsabbildungen $p_k : X \to X_k$ stetig sind, sind die Bilder zusammenhängender Teilmengen aus X zusammenhängend in X_k. Liegen daher zwei Elemente x, y aus X in ein und derselben Zusammenhangskomponente, dann sind deren Projektionen gleich. Somit gilt, weil die X_k total unzusammenhängend sind, $x = y$.

Damit ist (5.5) bewiesen.

Gelegentlich ist eine kategorielle Betrachtungsweise projektiver und induktiver Grenzwerte nützlich. Wir stellen diese Sichtweise nachfolgend kurz dar und folgen dabei den entsprechenden Ausführungen in [KC]. Dazu betrachten wir die bezüglich der Ordnungsrelation $\leq$ gerichtete Menge I als Kategorie: Die Objekte sind die Elemente von I und für $i, j \in I$ ist

$$Mor(i,j) := \begin{cases} \{\leq\}, \text{ falls } i \leq j \\ \emptyset, \text{ andernfalls} \end{cases}$$

die Menge der Morphismen von i nach j. Sei $\mathfrak{A}$ eine Kategorie. Ein projektives (inverses) System von $\mathfrak{A}$ über I läßt sich dann auffassen als kontravarianter Funktor $P : I \to \mathfrak{A}$; wir schreiben

$$P = (I, X_i, f_{ij})$$

mit

$$X_i = P(i),\ i \in I;\ \ f_{ij} = P(i \leq j) : X_j \to X_i,\ i, j \in I,\ i \leq j.$$

Ein direktes System von I über $\mathfrak{A}$ ist ein kovarianter Funktor $P : I \to \mathfrak{A}$; wir schreiben

$$P = (I, X_i, f_{ij})$$

mit

$$X_i = P(i),\ i \in I,\ \ f_{ij} = P(i \leq j) : X_i \to X_j,\ \ i, j \in I,\ i \leq j.$$

Sei X ein Objekt von $\mathfrak{A}$. Das sogenannte triviale inverse System P ordnet jedem $i \in I$ das Objekt X zu und ordnet dem Morphismus, der $i \leq j$ entspricht, die Identität von X zu. Jedem Morphismus $f : X' \to X$ von $\mathfrak{A}$ entspricht ein Morphismus von Funktoren $P_{X'} \to P_X$, der ebenfalls mit f bezeichnet wird. Ist $P = (I, X_i, f_{ij})$ ein projektives System von $\mathfrak{A}$ über I, dann ist der projektive (inverse) Grenzwert von P, falls es existiert, ein Objekt X von $\mathfrak{A}$ zusammen mit einem Morphismus von Funktoren $\Phi : P_X \to P$, so daß für jedes Objekt X' von $\mathfrak{A}$ und für jeden Morphismus von Funktoren $\Phi' : P_{X'} \to P$ genau ein Morphismus $f : X' \to X$ existiert, so daß $\Phi \circ f = \Phi'$. Dabei ist ein Morphismus von Funktoren $P_X \to P$ gegeben durch eine Familie von Morphismen $(\varphi_i : X \to X_i)_{i \in I}$, so daß für alle $i, j \in I$ mit $i \leq j$ das folgende Diagramm kommutiert

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$$\begin{array}{ccc} X & \xrightarrow{\varphi_i} & X_i \\ \varphi_j \searrow & & \nearrow f_{ij} \\ & X_j & \end{array}$$

Sind $P = (I, X_i, f_{ij})$ bzw. $Q = (J, Y_i, g_{ij})$ projektive Systeme von der Kategorie $\mathfrak{A}$ über I bzw. J, dann ist ein Morphismus $\Psi : P \to Q$ ein Morphismus $\Phi : J \to I$ zusammen mit einer Familie von Morphismen

$$\Psi_j : X_{\Phi(j)} \to Y_j, \;\; j \in J,$$

so daß für alle $i, j \in J$ mit $i \leq j$ das folgende Diagramm kommutiert

$$\begin{array}{ccc} X_{\Phi(j)} & \xrightarrow{\Psi_j} & Y_j \\ f_{\Phi(i),\Phi(j)} \downarrow & & \downarrow g_{ij} \\ X_{\Phi(i)} & \xrightarrow{\Psi_i} & X_i \end{array}$$

Ein solcher Morphismus $\Psi : P \to Q$ induziert einen Morphismus der entsprechenden projektiven Grenzwerte

$$\varphi : \varprojlim X_i \to \varprojlim Y_i, \;\; \varphi(\prod_{i \in I} x_i) := \prod_{j \in I} \Psi_j(x_{\Phi(j)}).$$

Sei $\mathfrak{A}_I$ die Kategorie der projektiven Systeme von der Kategorie $\mathfrak{A}$ über I. Für den Beweis des folgenden Satzes verweisen wir auf $[KC]$, 1.1.

(5.6) **Satz** *Der Funktor*

$$\varprojlim_{i \in I} : \mathfrak{A}_I \to \mathfrak{A}$$

ist exakt, d.h. sind $W := (I, W_i, e_{ij})$, $X := (I, X_i, f_{ij})$, $Y := (I, Y_i, g_{ij})$ *Objekte von* $\mathfrak{A}_I$, *sind* $W \to X$, $X \to Y$ *Morphismen in* $\mathfrak{A}_I$ *und ist für jedes* $i \in I$ *die zugehörige Sequenz von Morphismen*

$$1 \to W_i \to X_i \to Y_i \to 1$$

in $\mathfrak{A}$ *exakt, dann ist auch die folgende Sequenz von Morphismen in* $\mathfrak{A}$ *exakt*

$$1 \to \varprojlim W_i \to \varprojlim X_i \to \varprojlim Y_i \to 1.$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Aufgaben und Beispiele

(1) Sei $f : X \to Y$ eine stetige Abbildung von topologischen Räumen. Zeigen Sie: Ist $U \subset X$ eine kompakte Teilmenge und ist die Topologie von Y diskret, dann ist die Menge $f(U)$ endlich. (Ganz einfach)

(2) Geben Sie einen Beweis für Satz (5.6). (Vgl. [KC], 1.1)

§ 6. Proendliche Gruppen

In diesem Abschnitt werden grundlegende Tatsachen über proendliche Gruppen zusammengestellt. Dabei folgen wir entsprechenden Ausführungen in [GB]; [$H1$], 2.4.2; [KC]; [RB]; [$SE2$], Chapter I; [SH] bzw. [WS].

Eine *topologische Gruppe* ist eine Gruppe G, die ein topologischer Raum ist, so daß die Gruppenoperationen

$$G \times G \to G\ ,\ (a,b) \mapsto ab; \quad G \to G\ ,\ a \mapsto a^{-1}$$

stetige Abbildungen sind; dabei wird $G \times G$ als topologischer Raum bezüglich der Produkttopologie betrachtet (siehe § 5). Die topologischen Gruppen - als Objekte - zusammen mit den stetigen Gruppenhomomorphismen - als Morphismen - bilden eine Kategorie.

(6.1) **Satz** *Seien G, G' topologische Gruppen. Dann gilt:*

(i) Ist $U \subset G$ offen und ist $A \subset G$ eine beliebige Teilmenge, so sind AU und UA offen

(ii) Ist $f : G \to G'$ ein Homomorphismus von abstrakten Gruppen, dann ist f stetig, wenn jede Menge einer Umgebungsbasis des neutralen Elementes von G' ein offenes Urbild besitzt.

Beweis: (i) Für festes $s \in G$ sind die Abbildungen

$$t_s : G \to G\ ,\ t \mapsto ts^{-1};\ \ s^t : G \to G\ ,\ t \mapsto s^{-1}t$$

stetig, weil sie sich jeweils als Komposition von stetigen Abbildungen darstellen lassen. Deshalb sind die Urbilder von $U \subset G$, nämlich Us bzw. sU, jeweils offen. Somit sind die Mengen

$$UA = \cup_{s \in A} Us \ \text{ bzw. } \ AU = \cup_{s \in A} sU$$

jeweils als Vereinigung offener Mengen offen.

(ii) Wenn offene Teilmengen $G_i \subset G'$ eine Umgebungsbasis des neutralen Elementes von G' bilden, dann bilden für jedes $s \in G'$ die nach (i) offenen Teilmengen sG_i eine Umgebungsbasis von s; denn wenn U eine Umgebung von s ist, dann ist $s^{-1}U$ eine Umgebung des neutralen Elementes; und ist $G_k \subset s^{-1}U$ eine Menge aus einer Umgebungsbasis des neutralen Elementes, dann ist $sG_k \subset ss^{-1}U = U$ eine offene Teilmenge. Die Behauptung folgt.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Damit ist (6.1) bewiesen.

Mit den Methoden aus § 5 läßt sich der folgende Satz beweisen.

(6.2) **Satz** *In der Kategorie der topologischen Gruppen existieren stets Produkte und projektive Grenzwerte.*

Im Folgenden werden endliche Gruppen als diskrete topologische Gruppen betrachtet.

Definition Eine *proendliche Gruppe* ist eine topologische Gruppe, die projektiver Grenzwert endlicher Gruppen ist.

Die proendlichen Gruppen als Objekte zusammen mit den stetigen Gruppenhomomorphismen als Morphismen bilden eine Kategorie.
Nachfolgend beschreiben wir einige Eigenschaften proendlicher Gruppen.

(6.3) **Satz** *Sei (I, G_i, f_{ij}) ein projektives System endlicher Gruppen und sei G der projektive Grenzwert dieses Systems. Seien $p_i : G \to G_i$ die entsprechenden Projektionsabbildungen. Dann ist G sowohl hausdorffsch als auch kompakt, und die Menge $\{Kern(p_i) : i \in I\}$ bildet eine Umgebungsbasis des neutralen Elementes von G, die aus lauter offenen Normalteilern von endlichem Index besteht. Außerdem ist G total unzusammenhängend.*

Beweis: Die endlichen, diskreten Gruppen G_i sind hausdorffsch und, da jede ihrer Überdeckungen endlich ist, auch kompakt. Nach (5.5) ist damit auch G hausdorffsch und kompakt. Die Normalteiler $Kern(p_i)$, $i \in I$, sind alle offen; denn in der diskreten Menge G_i sind die einelementigen Mengen $\{e_{G_i}\}$, die jeweils nur aus dem neutralen Element von G_i bestehen, offen, und daher sind wegen der Stetigkeit der p_i die Mengen $Kern(p_i)$ als Urbilder von $\{e_{G_i}\}$ unter den stetigen Projektionsabbildungen p_i ebenfalls offen. Sie haben nach Konstruktion auch endlichen Index. Es bleibt zu zeigen, daß $\{Kern(p_i) : i \in I\}$ eine Umgebungsbasis von 1_G ist und daß G total unzusammenhängend ist. Sei $V \subset G$ eine offene Umgebung von e_G und sei U eine offene Menge im topologischen Produktraum $\prod_{i \in I} G_i$ mit der Eigenschaft $V = U \cap G$. Dann gibt es nach Definition der Produkttopologie eine endliche Teilmenge $S \subset I$ und für jedes $i \in S$ eine offene Teilmenge $U_i \subset G_i$, so daß

$$U \supset \prod_{i \in S} U_i \times \prod_{i \in I \setminus S} G_i.$$

Sei $k \in I$ so, daß $i \leq k$ für alle $i \in S$. Wir zeigen, daß $Kern(p_k) \subset U$: Es ist

$$Kern(p_k) = \{(s_i)_{i \in I} \in G : s_k = e_{G_k}\} =$$

$$= \{(s_i)_{i \in I} \in \prod_{i \in I} G_i : s_k = e_{G_k} \text{ und } f_{ij}(s_j) = s_i \text{ für alle } i \leq j\}.$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Ist daher $(s_i)_{i\in I} \in Kern(p_k)$, dann gilt für alle $i \in S$ wegen $i \leq k$:

$$f_{ik}(e_{G_k}) = e_{G_i} = s_i \ ,$$

d.h. $s_i \in U_i$, weil U_i eine Umgebung von e_{G_i} ist; und für $i \in I \setminus S$ gilt $s_i \in G_i$. Somit ist $(s_i)_{i\in I} \in U$.

Damit ist $Kern(p_k)$ eine offene Teilmenge von U und wegen $Kern(p_k) \subset G$ auch eine offene Teilmenge von V. Somit bildet die Menge

$$\{Kern(p_i) : i \in I\}$$

eine Umgebungsbasis des neutralen Elementes e_G von G, die aus lauter offenen Normalteilern von endlichem Index besteht.

Die G_i sind als endliche Gruppen mit der diskreten Topologie total unzusammenhängend, und damit ist nach (5.5) auch G total unzusammenhängend.

Damit ist der Beweis von (6.3) beendet.

(6.4) **Satz** *G sei eine topologische Gruppe, die sowohl hausdorffsch als auch kompakt ist und eine Umgebungsbasis $\{N_i : i \in I\}$ des neutralen Elementes 1_G besitzt, die aus allen offenen Normalteilern N_i von G besteht. Dann haben alle N_i endlichen Index in G, und* es *gilt $G \cong G' := \varprojlim G/N_i$, wobei der projektive Grenzwert bezüglich der Projektionsabbildungen $p_{ij} : G/N_j \to G/N_i$ für $i, j \in I$ mit $N_j \subset N_i$, gebildet ist.*

Beweis: Wir zeigen zunächst, daß I mit der Festsetzung "$i \leq j$ genau dann, wenn $N_i \supset N_j$" zu einer geordneten, gerichteten Menge wird. Seien dazu $i, j \in I$. Da der Durchschnitt von zwei offenen Normalteilern N_i, N_j wieder ein offener Normalteiler ist, hat $k \in I$ mit $N_k := N_i \cap N_j$ die Eigenschaft $i \leq k$ und $j \leq k$. Aus der vorausgesetzten Kompaktheit von G folgt, daß die Faktorgruppen G/N_i, $i \in I$, alle endlich sind; denn G ist disjunkte Vereinigung der nach (6.1), (i), offenen Nebenklassen von N_i in G, und endlich viele davon reichen aus, um G zu überdecken. Die Faktorgruppen G/N_i, $i \in I$, sind bezüglich der Quotiententopologie topologische Gruppen. Sind sN_i und $s'N_i$ zwei verschiedene Elemente aus G/N_i, dann existiert eine offene Umgebung U von s und eine offene Umgebung U' von s' in G, so daß $U \cap U' = \emptyset$; denn G ist nach Voraussetzung hausdorffsch. Somit sind $V := U \cap sN_i$ und $V' := U' \cap s'N_i$ disjunkt und offen in G. Also sind VN_i und $V'N_i$ disjunkte und nach (6.1), (i), offene Umgebungen von sN_i bzw. $s'N_i$ in G/N_i. Die Faktorgruppen G/N_i, $i \in I$, sind somit alle hausdorffsch und wegen ihrer Endlichkeit auch diskret. Ist $N_j \subset N_i$ und UN_i offen in G/N_i, dann ist nach Definition der Quotiententopologie auch U offen. Also ist UN_j offen in G/N_j. Wegen $UN_j = p_{ij}^{-1}(UN_i)$ sind die Projektionsabbildungen $p_{ij} : G_j \to G_i$ alle stetig. $(I, G/N_i, p_{ij})$ ist also ein projektives System. Es ist noch zu zeigen, daß die folgende Abbildung ein Isomorphismus und ein Homöomorphismus ist:

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$f : G \to G' := \varprojlim G/N_i, \;\; s \mapsto (sN_i)_{i\in I}.$

Wegen $f(st) = (stN_i)_{i\in I} = (sN_itN_i)_{i\in I}$ ist f ein Homomorphismus. Außerdem folgt aus der Definition, daß $Kern(f) = \cap_{i\in I}N_i$. Wir zeigen $\cap_{i\in I}N_i = \{e_G\}$. Angenommen es existiert ein $s \in G$, $s \neq 1_G$ mit $s \in \cap_{i\in I}N_i$. Da G hausdorffsch ist, existiert eine Umgebung von s, die disjunkt zu einer Umgebung U von e_G ist. Sei N ein offener Normalteiler von G mit $N \subset U$, etwa $N = N_k$. Ein solches N existiert, da die N_i, $i \in I$, nach Voraussetzung eine Umgebungsbasis von e_G bilden. Dann ist $s \notin N_k$ und somit $s \notin \cap_{i\in I}N_i$, im Widerspruch zur Wahl von s. Also ist f injektiv. Wir betrachten nun die Projektionsabbildungen

$p_k : G \to G/N_k \;\;, \;\; s \mapsto sN_k$

$p'_k : G' \to G/N_k \;, \;\; (sN_i)_{i\in I} \mapsto sN_k \;.$

Nach Definition der Quotiententopologie ist p_k stetig, und p'_k ist stetig aufgrund der Definition der Produkttopologie. Nach (6.3) ist $\{Kern(p'_i) : i \in I\}$ eine Umgebungsbasis des neutralen Elementes $e_{G'}$ von G', die aus lauter offenen Mengen besteht. Das Urbild von $Kern(p'_k)$ unter f ist N_k, also offen, also f stetig. Sei $s := (s_i)_{i\in I} \in G'$. Dann ist $sKern(p'_k)$ eine offene Umgebung von s. Sei $t \in s_kN_k \subset G$. Dann ist $f(t) \in sKern(p'_k)$. Daraus folgt, daß das Bild $f(G)$ von f dicht in G' liegt. Da G kompakt ist, ist $f(G)$ kompakt und abgeschlossen, also $f(G) = \overline{f(G)} = G'$. f ist also auch surjektiv. Insgesamt ist damit bewiesen, daß f ein Isomorphismus ist. Ist $A \subset G$ abgeschlossen, dann ist A und damit $f(A)$ kompakt. Also ist $f(A)$ auch abgeschlossen. Es folgt, daß auch die Umkehrabbildung von f stetig und damit f ein Homöomorphismus ist. Damit ist (6.4) bewiesen.

Wir halten ausdrücklich fest, daß offene Untergruppen proendlicher Gruppen endlichen Index besitzen, weil die offene Überdeckung einer proendlichen Gruppe G, die durch eine Nebenklassenzerlegung nach einer offenen Untergruppe gegeben wird, wegen der Kompaktheit von G eine endliche Teilüberdeckung enthält. Außerdem ist jede offene Untergruppe U einer proendlichen Gruppe als Komplement der offenen Menge, die durch die Vereinigung der von U verschiedenen Nebenklassen von U gegeben wird, auch abgeschlossen. Ist U eine abgeschlossene Untergruppe einer proendlichen Gruppe und hat U endlichen Index in G, dann ist U als Komplement der abgeschlossenen Menge, die durch die Vereinigung der von U verschiedenen Nebenklassen von U gegeben wird, auch offen.

Es läßt sich zeigen, daß abgeschlossene Untergruppen, Faktorgruppen nach abgeschlossenen Normalteilern, direkte Produkte bzw. projektive Grenzwerte von proendlichen Gruppen wieder proendliche Gruppen sind. Außerdem ist für jede abgeschlossene Untergruppe H der proendlichen Gruppe G der homogene

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Raum $G \setminus H$ aller Rechtsnebenklassen von H in G kompakt und total unzusammenhängend ist.

Die Existenz stetiger Repräsentantensysteme in proendlichen Gruppen wird durch den folgenden Satz garantiert; vgl. [$SE2$], Chapter I, 1.2.

(6.5) **Satz** *Sei H eine abgeschlossene Untergruppe der proendlichen Gruppe G. Dann existiert ein stetiges Repräsentantensystem $u : G \setminus H \to G$, $\sigma \mapsto u_\sigma$, mit $u(H) = e_G$, d.h. u ist eine stetige Abbildung von der Menge der Rechtsnebenklassen von H in G, die die Nebenklasse H auf das neutrale Element e_G von G abbildet, so daß die Komposition von u mit der Projektionsabbildung $G \to G \setminus H$ die identische Abbildung ist.*

Allgemeiner gilt, vgl. [$SE2$], Chapter I, 1.2

(6.6) **Satz** *Seien $K \subset H$ abgeschlossene Untergruppen der proendlichen Gruppe G. Dann existiert ein stetiger Schnitt $s : G \setminus H \to G \setminus K$, d.h. eine stetige Abbildung s von dem topologischen Raum der Rechtsnebenklassen von H in G in den topologischen Raum der Rechtsnebenklassen von K in G, so daß die Komposition von s mit der durch $K \subset H$ induzierten Projektionsabbildung $G \setminus K \to G \setminus H$ die Identität ergibt.*

Wir folgen beim Beweis dieses Satzes der Darstellung in [$SE2$], Chapter I, §1, und beweisen zunächst zwei Hilfssätze.

(6.7) **Hilfssatz** *Sei G eine kompakte Gruppe und sei $(S_i)_{i\in I}$ eine absteigende Folge von abgeschlossenen Untergruppen S_i, so daß also $(I, G \setminus S_i, f_{ij})$ mit der durch $S_j \subset S_i$ induzierten Projektionsabbildung $f_{ij} : G \setminus S_j \to G \setminus S_i$, $xS_j \mapsto xS_i$, ein projektives System topologischer Räume bildet. Sei $S := \cap_{i\in I} S_i$. Dann ist die Abbildung*

$$f : G \setminus S \to \varprojlim G \setminus S_i \ , \ xS \mapsto (xS_i)_{i\in I} \ ,$$

ein Homöomorphismus topologischer Räume.

Beweis: Die Abbildung f ist nach Konstruktion stetig und injektiv, und ihr Bild liegt dicht. Da G und alle Quotientenräume kompakt sind und somit auch der projektive Grenzwert kompakt ist, ist auch $Bild(f)$ kompakt, also abgeschlossen, und damit $\varprojlim G \setminus S_i = \overline{Bild(f)} = Bild(f)$, also f surjektiv. Ist $A \subset G \setminus S$ abgeschlossen, dann ist A und damit auch $f(A)$ kompakt und daher abgeschlossen. Die Umkehrabbildung von f ist also stetig. f ist somit ein Hmöomorphismus.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

(6.8) **Hilfssatz** *Der Satz ist richtig, wenn $H \setminus K$ endlich ist. Wenn H und K Normalteiler von G sind, dann zerfällt die exakte Sequenz $1 \to H/K \to G/K \to G/H \to 1$ auf einer offenen Untergruppe von G/H.*

Beweis: Sei U ein offener Normalteiler von G mit $U \cap H \subset K$. Die Einschränkung der Projektionsabbildung $\pi : G/K \to G/H,\ \ xK \mapsto xH$, auf das Bild U' von U in G/K ist also injektiv und ein Homomorphismus, wenn H und K Normalteiler sind. Sei $U" := \pi(U')$. Die Umkehrabbildung $s := (\pi_{|U'})^{-1} : U" \to U'$ ist ein Schnitt. Daraus folgt die Behauptung über das Zerfallen der exakten Sequenz auf der offenen Untergruppe $U' \subset G/H$. Weil $U"$ offen in der kompakten Gruppe G/H ist, hat $U"$ in G/H endlichen Index. Mit Hilfe einer endlichen Nebenklassenzerlegung $G/H = \dot\cup_x xU"$ läßt sich dieser Schnitt s zu einem Schnitt auf G/H fortsetzen:

$s'(xu) := xs(u),\ u \in U"$.

Damit ist (6.8) bewiesen.

Beweis von (6.6): Wir können ohne Einschränkung annehmen, daß $K = \{1\}$ ist. Sei X die Menge aller Paare (S, s), wobei S eine abgeschlossene Untergruppe von H und $s : G \setminus H \to G \setminus S$ ein stetiger Schnitt ist. X wird wie folgt geordnet: Es gilt $(S', s') \leq (S, s)$ genau dann, wenn $S \subset S'$ und wenn s' die Komposition des Schnittes $s : G \setminus H \to G \setminus S$ mit der Projektionsabbildung $G \setminus S \to G \setminus S'$ ist. Sei $\{(S_i, s_i)\}_{i \in I}$ eine total geordnete Teilmenge von X und sei $S := \cap_{i \in I} S_i$. S' ist eine abgeschlossene Untergruppe von H. Nach (6.8) ist $G \setminus S$ homöomorph zu $\varprojlim G \setminus S_i$. Aus den stetigen Schnitten $s_i : G \setminus H \to G \setminus S_i$ erhält man daher einen stetigen Schnitt $s : G \setminus H \to G \setminus S$, d.h. es gilt $(S, s) \in X$. Das Lemma von Zorn hat zur Folge, daß X ein maximales Element (T, t) enthält: Wir zeigen, daß $T = \{1\}$ ist. Angenommen $T \neq \{1\}$. Dann existiert eine offene Untergruppe U von G, so daß $T \cap U \neq T$. Hilfssatz (6.9), angewandt auf $(G, T, T \cap U)$, liefert einen stetigen Schnitt $G \setminus T \to G \setminus (T \cap U)$. Der Schnitt $t : G \setminus H \to G \setminus T$ komponiert mit diesem Schnitt ergibt einen stetigen Schnitt $G \setminus H \to G \setminus (T \cap U)$, im Widerspruch zur Maximalität von (T, t).
Damit ist der Beweis von (6.7) beendet.

Sei I eine Menge und sei $F(I)$ die freie Gruppe mit freien Erzeugern s_i, $i \in I$. Sei $\mathcal{N}$ die Menge aller Normalteiler von $F(I)$ von endlichem Index, die fast alle s_i enthalten. Man erhält ein projektives System

$(\mathcal{N}, F(I)/N, f_{N,M})$,

wobei für $M, N \in \mathcal{N}$ mit $M \subset N$

$f_{N,M} : F(I)/M \to F(I)/N$

die durch $M \subset N$ induzierte Projektionsabbildung ist. Der projektive Grenzwert dieses Systems

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$F_I := \varprojlim_{N \in \mathcal{N}} F(I)/N$

heißt die *freie proendliche Gruppe mit freien Erzeugern* $s_i, i \in I$.

Ist $\mathcal{N}$ die Familie aller Normalteiler von $F(I)$ von endlichem Index mit auflösbarer Faktorgruppe bzw. mit Faktorgruppe von p-Potenzindex für eine Primzahl p, die jeweils fast alle s_i enthalten, dann heißt der entsprechende projektive Grenzwert F_I die *freie proauflösbare* bzw. die *freie pro-p-Gruppe mit freien Erzeugern* $s_i, i \in I$.

Der folgende Satz wird z.B. in $[KC]$ bewiesen.

(6.9) **Satz** *In allen drei Fällen ist die natürliche Abbildung* $F(I) \to F_I$ *injektiv. Ist* G *eine proendliche Gruppe und ist* $\{g_i : i \in I\}$ *eine Menge von Elementen aus* G, *so daß jede Umgebung des neutralen Elementes von* G *fast alle* g_i *enthält, dann induziert die Zuordnung* $s_i \longmapsto g_i, i \in I$, *einen stetigen Homomorphismus* $F_I \to G$.

Definition Sei G eine proendliche Gruppe. Eine Menge von Elementen $A = \{g_i : i \in I\}$ aus G heißt *Erzeugendensystem* von G, wenn die kleinste abgeschlossene Untergruppe von G, die A enthält, gleich G ist, d.h. wenn G gleich dem Durchschnitt aller abgeschlossenen Untergruppen U von G mit $A \subset U$ ist.

Aufgaben und Beispiele

(1) Sei $\mathbb{P}$ die Menge aller Primzahlen. Die Elemente von

$\widetilde{\mathbb{N}}_0 := \{f : \mathbb{P} \to \mathbb{N}_0 \cup \{\infty\} \text{ Abbildung}\}$

$= \{ \prod_{p \in \mathbb{P}} p^{m_p} : m_p \in \mathbb{N}_0 \cup \{\infty\}\}$

heißen "übernatürliche Zahlen"; Produkte, größte gemeinsame Teiler sowie kleinste gemeinsame Vielfache von Elementen aus $\widetilde{\mathbb{N}}_0$ sind in offensichtlicher Weise definiert. Sei G eine proendliche Gruppe und sei H eine abgeschlossene Untergruppe von G. Der Index von H in G ist definiert durch

$(G : H) := kgV\{G/U : H/(H \cap U)),\ U \text{ offener Normalteiler in } G\}.$

Zeigen Sie: Sind $K \leq H \leq G$ proendlich, dann gilt

$(G : H) = (G : H)(H : K)$

und H ist genau dann offen in G, wenn$(G : H) \in N$.

Insbesondere ist also der Begriff "Ordnung von G" definiert. (Vgl. $[SE2]$, Chapter I, §1)

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

(2) Sei G eine proendliche Gruppe und sei $\mathbb{Q}/\mathbb{Z}$ mit der diskreten Topologie versehen. Sei $\chi : G \to \mathbb{Q}/\mathbb{Z}$ ein stetiger Homomorphismus. Zeigen Sie: Die Faktorgruppe $G/Ker(\chi)$ ist eine endliche zyklische Gruppe. (Ziemlich leicht)

(3) Die Charaktergruppe einer proendlichen Gruppe: Sei G eine proendliche Gruppe und sei $\chi : G \to \mathbb{R}/\mathbb{Z}$ ein stetiger Homomorphismus von G in die topologische Faktorgruppe der additiven Gruppe von $\mathbb{R}$ modulo der additiven Gruppe von $\mathbb{Z}$. Mit G ist auch das Bild von χ eine kompakte und total unzusammenhängende Gruppe. Daraus folgt, daß das Bild von χ eine endliche Untergruppe von $\mathbb{Q}/\mathbb{Z}$ ist. Da jede endliche Untergruppe von $\mathbb{Q}/\mathbb{Z}$ zyklisch ist, ist somit das Bild von χ eine endliche zyklische Gruppe, die nach dem ersten Isomorphiesatz der Gruppentheorie isomorph zu $G/Kern(\chi)$ ist. Insbesondere ist die Gruppe aller stetigen Homomorphismen

$$\widehat{G} := Hom(G, \mathbb{R}/\mathbb{Z}),$$

das sogenannte *Pontrjagin-Dual von G* oder die *Charaktergruppe von G*, eine diskrete abelsche Torsionsgruppe. Jeder stetige Homomorphismus $f : G \to G'$ von proendlichen Gruppen induziert einen dazu "dualen" stetigen Homomorphismus der Charaktergruppen

$$\widehat{f} : \widehat{G'} \to \widehat{G}\ ,\ \widehat{f}(\chi)(g) := \chi(f(g))\ ;\ \ \chi \in \widehat{G}\ ,\ g \in G.$$

Die Zuordnung, die jeder proendlichen abelschen Gruppe ihr Pontrjagin-Dual und jedem stetigen Homomorphismus von proendlichen abelschen Gruppen den dazu dualen Homomorphismus zuordnet, erweist sich als ein exakter Funktor von der Kategorie der proendlichen abelschen Gruppen in die Kategorie der diskreten abelschen Torsionsgruppen, d.h. jede exakte Sequenz von stetigen Homomorphismen proendlicher abelscher Gruppen

$$1 \to H \to G \to G/H \to 1$$

induziert die dazu "duale exakte Sequenz"

$$1 \to \widehat{G/H} \to \widehat{G} \to \widehat{H} \to 1$$

(Vgl. $[KC]$, §1)

§ 7. Unendliche Galoiserweiterungen

In diesem Abschnitt formulieren wir die Galoistheorie für Körpererweiterungen, die nicht notwendigerweise endlichen Grad besitzen und folgen dabei weitgehend den entsprechenden Darstellungen in $[SW]$, Appendix, A2.3; $[WS]$, section 3; vgl. auch $[H1]$, 2.4.5.

Sei k ein Körper und sei Ω/k eine Galoiserweiterung mit Galoisgruppe $G = G(\Omega/k)$ Wir setzen nicht voraus, daß der Grad von Ω über k endlich ist. Mit Methoden der Galoistheorie endlicher Körpererweiterungen und unter

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Zuhilfenahme des Zornschen Lemmas beweist man das folgende Resultat, vgl. $[SW]$, A2.3, Lemma A.8 oder $[WS]$, section 3.

(7.1) **Satz** *Die Zuordnung, die jedem Zwischenkörper L von Ω/k die Untergruppe $H := H_L := \{s \in G : s(x) = x$ für alle $x \in L\}$ zuordnet, ist eine injektive Abbildung von der Menge aller Zwischenkörper von Ω/k in die Menge aller Untergruppen von G mit der Eigenschaft $H_L = G(\Omega/L)$.*

Außerdem beweist man in der Galoitheorie endlicher Körpererweiterungen, vgl. z.B. $[A]$, II; $[KU]$ oder $[LO1]$:

(7.2) **Satz** *Wenn Ω/k endlich ist, dann ist die in (7.1) beschriebene Zuordnung $L \mapsto H_L$ nicht nur injektiv, sondern auch surjektiv.*

Weiterhin gilt für jeden Zwischenkörper L von Ω/k

(7.3) $\quad G(\Omega/sL) = sG(\Omega/L)s^{-1}$ für alle $\quad s \in G;$

insbesondere ist L/k genau dann normal, wenn $H_L = G(\Omega/L)$ ein Normalteiler von G ist.

Im allgemeinen ist jedoch nicht jede Untergruppe von G Galoisgruppe von Ω über einem Zwischenkörper von Ω/k. Einer Bemerkung von R. Dedekind $[DK]$, S. 288, Zeilen 23-25, folgend, hat F. Krull $[KR]$ auf G eine Topologie eingeführt und gezeigt, daß die bezüglich dieser Topologie abgeschlossenen Untergruppen von G genau die Galoisgruppen von Ω über Zwischenkörpern von Ω/k sind. Diese Topologie führt man am besten durch Angabe von Umgebungsbasen ein. Dazu sei für jedes $s \in G$

$$\mathcal{U}(s) := \{sG(\Omega/K) : K/k \text{ endliche Galoiserweiterung in } \Omega\}$$

(7.4) **Satz** *(i) Für jedes $s \in G$ ist $\mathcal{U}(s)$ Umgebungsbasis einer Topologie auf G*

(ii) G ist bezüglich dieser Topologie eine proendliche Gruppe.

Beweis: Sei $\{K_i : i \in I\}$ die Menge aller endlichen Galoiserweiterungen K_i/k, $K_i \subset \Omega$, und sei $H_i := G(\Omega/K_i) \trianglelefteq G$, $G_i := G/H_i = G(K_i/k)$. Für $K_i \subset K_j$ sei $f_{ij} : G_j \to G_i$ der Restriktionsepimorphismus, der jeden k-Automorphismus von K_j auf K_i einschränkt. Dann ist (I, G, f_{ij}) ein projektives System endlicher Gruppen. Sei G' der projektive Grenzwert mit den Projektionsabbildungen $p_i : G' \to G_i$. Es gilt $G = G'$, und die p_i sind die Restriktionsepimorphismen, die die k-Automorphismen von Ω auf K_i einschränken. Um das einzusehen, sei $s \in G$. Jedes $x \in \Omega$ liegt in einer endlichen Galoiserweiterung K_i/k, und es gilt $(p_i \circ s)(x) = s(x)$. Also ist s durch die $p_i \circ s$, $i \in I$, eindeutig bestimmt. Die Behauptungen des Satzes ergeben sich nun aus (6.3).

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Wir beweisen nun die oben erwähnte Charakterisierung derjenigen Untergruppen von $G = G(\Omega/k)$, die Galoisgruppen von Zwischenkörpererweiterungen von Ω/k sind.

(7.5) **Hilfssatz** *Sei H eine Untergruppe von $G = G(\Omega/k)$. Genau dann existiert ein Zwischenkörper L von Ω/k mit $H = G(\Omega/L)$, wenn H eine abgeschlossene Untergruppe in der proendlichen Gruppe G ist.*

Beweis: Sei zunächst H von der Form $H = G(\Omega/L)$ für einen Zwischenkörper L von Ω/k. Sei $s \in G$ enthalten im topologischen Abschluß $\bar{H}$ von H in G. Es ist zu zeigen, daß $s(x) = x$ für alle $x \in L$ gilt. Sei $M \subset \Omega$ der Zerfällungskörper für das Minimalpolynom von x über k. M/k ist eine endliche Galoierweiterung. Seien $H_0 := G(\Omega/M)$, $G_0 := G(M/k)$ und sei $p_0 : G \to G_0$ die entsprechende Restriktionsabbildung. Da G_0 diskret ist, ist $p_0(H)$ abgeschlossen in G_0. x wird von allen Elementen aus $p_0(H)$ fest gelassen. Wegen der Stetigkeit von p_0 ist das Urbild $p_0^{-1}(p_0(H))$ von $p_0(H)$ unter p_0 abgeschlossen. Somit liegt s in der abgeschlossenen Menge $p_0^{-1}(p_0(H))$ und läßt x fest.

Sei umgekehrt $H \leq G$ eine abgeschlossene Untergruppe und sei

$$L := \{x \in \Omega : s(x) = x \quad \text{für alle} \quad s \in H\}$$

der zu H gehörige Fixkörper. Sei $s \in G \setminus H$. Zu zeigen ist, daß L Elemente enthält, die unter s nicht fest bleiben. Sei $sG(\Omega/K_1)$ ein Element aus der oben definierten Umgebungsbasis von s mit der Eigenschaft $sG(\Omega/K_1) \cap H = \emptyset$. Sei $\widetilde{K}_1$ der Fixkörper von $p_1(H) \leq G_1 = G(K_1/k)$. Dann gilt $\widetilde{K}_1 \subset L$, aber nicht alle Elemente von $\widetilde{K}_1$ werden von s fest gelassen.

Damit ist der Hilfssatz bewiesen.

Der sogenannte "Hauptsatz der Galoistheorie" für Galoiserweiterungen Ω/k, die nicht notwendigerweise endlichen Grad besitzen, läßt sich jetzt folgendermaßen formulieren.

(7.6) **Satz** *Die Zuordnung $L \mapsto H = H_L$, die jedem Zwischenkörper L der Galoiserweiterung Ω/k die Untergruppe*

$$H := H_L := \{s \in G : s(x) = x \quad \textit{für alle} \quad x \in L\} \leq G$$

zuordnet, ist eine bijektive Abbildung von der Menge aller Zwischenkörper L von Ω/k auf die Menge aller abgeschlossenen Untergruppen von G.

Es ist im allgemeinen nicht bekannt, ob jede Untergruppe von $G = G(\Omega/k)$, die endlichen Index besitzt, offen in G ist.

(7.7) **Beispiele** (a) Sei $k = \mathbb{F}_q$ der endliche Körper mit q Elementen und sei $\Omega = \overline{k}$ ein algebraischer Abschluß von k. Bekanntlich besitzt k zu jeder

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

natürlichen Zahl n genau einen Erweiterungskörper $k^{(n)} \subset \Omega$ vom Grad n, und die Galoisgruppe $G^{(n)} := G(k^{(n)}/k)$ ist zyklisch der Ordnung n und wird durch den Frobenius Automorphismus

$$\sigma : x \mapsto x^q$$

erzeugt. Die Abbildung

$$G^{(n)} \to \mathbb{Z}/n\mathbb{Z},\ \sigma^\nu \mapsto \nu \bmod n$$

ist ein Isomorphismus von $G^{(n)}$ mit der additiven zyklischen Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$. Außerdem gilt $k^{(m)} \supset k^{(n)}$ genau dann, wenn n ein Teiler von m ist. Der Restriktionsabbildung $f_{m,n} : G^{(m)} \to G^{(n)}$ entspricht dabei die Abbildung $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, die ν mod m auf ν mod n abbildet. Wenn m und n teilerfremd sind, dann ist der Grad des Kompositums $k^{(m)}k^{(n)}$ innerhalb Ω gleich mn, also ist $k^{(m)}k^{(n)} = k^{(mn)}$. Außerdem ist die Abbildung $G^{(mn)} \to G^{(m)} \times G^{(n)}$, die jedem $s \in G^{(mn)}$ das 2-Tupel der Restriktionen $(s_{|k^{(m)}}, s_{|k^{(n)}}) \in G^{(m)} \times G^{(n)}$ zuordnet, ein Isomorphismus, der dem Isomorphismus $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ entspricht. Der projektive Grenzwert $G = \varprojlim G^{(n)}$ ist daher isomorph zum Produkt der projektiven Grenzwerte der $G^{(p^i)} \cong \mathbb{Z}/p^i\mathbb{Z}$, p Primzahl; letztere sind gleich der additiven Gruppe des Ringes $\mathbb{Z}_p$ aller p-adischen ganzen Zahlen, vgl. Beispiel (5.2),(a). Also ist

$$G \cong \prod\nolimits_{p \text{ Primzahl}} (\mathbb{Z}_p, +).$$

(b) Sei $k = \mathbb{Q}$ und $\Omega = \mathbb{Q}(e^{2\pi i/n} : n \in \mathbb{N})$ die Körperweiterung von $\mathbb{Q}$, die aus $\mathbb{Q}$ durch Adjunktion aller komplexen Einheitswurzeln entsteht. Bekanntlich existiert für jedes $n \in \mathbb{N}$ ein Isomorphismus $G(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ und daher - wegen $(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ für teilerfremde m, n - ein Isomorphismus

$$G \cong \prod\nolimits_{p \text{ Primzahl}} \mathbb{Z}_p^*,$$

wobei $\mathbb{Z}_p^* = \varprojlim (\mathbb{Z}/p^i\mathbb{Z})^*$ die Einheitengruppe des Ringes aller p-adischen ganzen Zahlen bezeichnet.

Aufgaben und Beispiele

(1) Geben Sie ausführliche Beweise für die in (7.7) gemachten Aussagen. (Vgl. z.B. [SW], A2.3, oder [WS])

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

§ 8. Stetige Operationen von proendlichen Gruppen und Kohomologie

In diesem Abschnitt erläutern wir die Kohomologie von proendlichen Gruppen und folgen dabei entsprechenden Darstellungen in $[GB]$; $[H1]$, 2.4.3 und 2.4.4; $[KC]$, $[KP]$, $[SH]$ und $[SE2]$.

Sei G eine proendliche Gruppe.

Definition Eine Menge A, die als topologischer Raum mit der diskreten Topologie betrachtet wird, heißt *diskrete Links-G-Menge*, wenn A eine Links-G-Menge ist und wenn die Abbildung

$$G \times A \to A,\ (s,a) \mapsto s(a) = a^s,$$

die dieser Operation entspricht, stetig ist; dabei ist $G \times A$ der topologische Produktraum. Eine Links-G-Gruppe A, die mit der diskreten Topologie versehen ist, heißt *diskrete Links-G-Gruppe*, wenn die Abbildung $G \times A \to A$, die der Operation von G auf A entspricht, stetig ist; ist A zusätzlich abelsch, dann heißt A ein *diskreter G-Modul*.

(8.1) **Satz** *Die folgenden Aussagen sind aequivalent*

(i) *A ist eine diskrete Links-G-Menge.*

(ii) *Für jedes $a \in A$ ist die Fixgruppe von a, also $G_a := \{s \in G : s(a) = a\}$ eine offene Untergruppe von G.*

(iii) *Ist $\mathcal{N}$ die Menge aller offenen Normalteiler von G, dann gilt $A = \cup_{N \in \mathcal{N}} A^N$*

(8.2) **Beispiel** Sei A eine Menge, auf der G trivial operiert, d.h. $s(a) = a$ für alle $s \in G$ und alle $a \in A$. Dann ist A eine diskrete G-Menge. Ist A eine Gruppe, auf der G trivial operiert, dann ist A eine diskrete G-Gruppe.

Bevor wir den Beweis von (8.1) durchführen, beschreiben wir die Stetigkeit der Operation

$$\gamma : G \times A \to A$$

etwas anders. Wegen der zugrundeliegenden diskreten Topologie auf A und aufgrund der Definition der Stetigkeit bedeutet sie, daß das Urbild jeder Teilmenge $U \subset A$ unter γ, also

$$\gamma^{-1}(U) = \{(s,a) \in G \times A : s(a) \in U\} =$$

$$= \cup_{a \in A}(\{s \in G : s(a) \in U\} \times \{a\}),$$

offen in $G \times A$ ist. Das wiederum ist aequivalent dazu, daß für jede Teilmenge $U \subset A$ die Mengen

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$$\{s \in G : s(a) \in U\}, \ \ a \in A,$$

offen in G sind.

Beweis von (8.1): Wir zeigen zunächst, daß aus der Aussage (i) die Aussage (ii) folgt. Sei dazu A eine diskrete G-Menge. Dann ist nach der Vorbemerkung für jede Teilmenge $U \subset A$ und jedes Element $a \in A$ die Menge

$$\{s \in G : s(a) \in U\}$$

offen in G. Insbesondere ist für $U = \{a\}$, $a \in A$, die Menge

$$\{s \in G : s(a) = a\}$$

offen in G. Also ist (ii) erfüllt.
Sei umgekehrt (ii) erfüllt. Sei $a \in A$. Dann ist auch die Urbildmenge

$$\gamma^{-1}(\{a\}) = G_a \times \{a\}$$

offen in $G \times A$. Und für eine beliebige Teilmenge $U \subset A$ ist daher die Urbildmenge

$$\gamma^{-1}(U) = \cup_{a \in U}(G_a \times \{a\})$$

als Vereinigung offener Mengen ebenfalls offen in $G \times A$. Also ist (i) erfüllt.

Wir zeigen nun, daß aus Aussage (ii) die Aussage (iii) folgt. Sei also G_a für alle $a \in A$ offen in G. Dann ist G_a in G als Komplement der Vereinigung der von G_a verschiedenen offenen Nebenklassen von G_a abgeschlossen, und der Index n von G_a in G ist wegen der Kompaktheit von G endlich. Ist $g_1, ..., g_n$ ein Repräsentantensystem der Rechtsnebenklassen von G_a in G, dann sind $g_1 a, ..., g_n a$ die paarweise verschiedenen Transformierten von a unter G. Man erhält also durch $g \to (g_i a \to g g_i a)$ einen Homomorphismus $G \to S_n$ von G in die symmetrische Gruppe S_n vom Grad n mit dem Kern

$$N := \cap_{i=1,\ldots,n} g_i G_a g_i^{-1} \ .$$

N ist als Kern eines Homomorphismus eine normale Untergruppe von G und als Durchschnitt endlich vieler offener Untergruppen von G offen in G. Außerdem gilt $a \in A^N$. Somit ist gezeigt, daß

$$A = \cup_{N \in \mathcal{N}} A^N.$$

Schließlich zeigen wir, daß Aussage (iii) die Aussage (i) zur Folge hat. Sei dazu $a \in A$ und sei N ein offener Normalteiler von G, so daß $a \in A^N$. Dann gilt $N \leq G_a$. Also ist G_a offen.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Damit ist der Beweis von (8.1) beendet.

Die Paare (G, A), wobei G eine proendliche Gruppe und A eine diskrete G-Gruppe ist, bilden die Objekte einer Kategorie $\mathfrak{K}$, deren Morphismen Paare

$$(\varphi, \psi) : (G, A) \to (G^{'}, A^{'})$$

von stetigen Gruppenhomomorphismen

$$\varphi : G' \to G \text{ und } \ \psi : A \to A^{'}$$

sind, so daß

$$s(\psi(a)) = \psi(\varphi(s)(a)) \ \text{ für alle } a \in A \text{ und alle } s \in G'.$$

Ist $(I, (G_i, A_i), (\varphi_{ij}, \psi_{ij}))$ ein induktives System von $\mathfrak{K}$ über I, dann ist (I, G_i, φ_{ij}) ein projektives System proendlicher Gruppen G_i, und (I, A_i, ψ_{ij}) ist ein induktives System diskreter Gruppen A_i. Sei

$$G := \varprojlim G_i \ \text{ und } \ A := \varinjlim A_i$$

der entsprechende projektive bzw. induktive Grenzwert. Aufgrund der Konstruktion des induktiven Grenzwertes (vgl. §5) ist $a \in A_i$ aequivalent zu $b \in A_j$ genau dann, wenn ein $k \in I$ mit $i \leq k, j \leq k$ existiert, so daß $\psi_{ik}(a) = \psi_{jk}(b)$. Im folgenden wird die Aequivalenzklasse von $a \in A_i$ innerhalb A mit $\overline{a}$ bezeichnet.

(8.3) **Satz** *A ist eine diskrete G-Gruppe, und, wenn alle A_i abelsch sind, ein diskreter G-Modul.*

Beweis: A ist bezüglich der folgenden Verknüpfung eine Gruppe:

$$A \times A \to A, \ (\overline{a}, \overline{b}) \mapsto \overline{\psi_{ik}(a)\psi_{jk}(b)},$$

wobei $a \in A_i, b \in A_j$ und $k \in I$ so ist, daß $i \leq k, j \leq k$. Um zu sehen, daß dadurch eine Abbildung wohldefiniert ist, sei $a' \in A_{i'}$ und sei $m \in I$ so, daß $i \leq m, i' \leq m$ und $\psi_{im}(a) = \psi_{i'm}(a')$; sei weiterhin $k^{'} \in I$ so, daß $i' \leq k', j \leq k'$ und sei $n \in I$ so, daß $k \leq n, k' \leq n, m \leq n$. Dann gilt

$$\psi_{in}(a) = \psi_{mn}(\psi_{im}(a)) = \psi_{mn}(\psi_{i'm}(a')) = \psi_{i'n}(a')$$

und

$$\psi_{kn}(\psi_{ik}(a)\psi_{jk}(b)) = \psi_{kn}(\psi_{ik}(a))\psi_{kn}(\psi_{jk}(b)) =$$

$$= \psi_{in}(a)\psi_{jn}(b) = \psi_{k'n}(\psi_{ik'}(a))\psi_{k'n}(\psi_{jk'}(b)) =$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$$= \psi_{k'n}(\psi_{ik'}(a^{'})\psi_{jk'}(b)).$$

Also ist $\overline{ab} = \overline{a'b}$.

Ein Repräsentant des neutralen Elementes in A ist jedes neutrale Element in einer der Gruppen A_i, d.h. $e_A = \overline{e}_{A_i}$; denn ist $a \in A_j$ und $k \in I$ so, daß $i \leq j, j \leq k$, dann ist

$$\psi_{ik}(a)\psi_{jk}(e_{A_j}) = \psi_{ik}(a)e_{A_k} = \psi_{ik}(a).$$

Auch die Inversenabbildung ist unabhängig von der Wahl eines Repräsentanten; denn sind a, a' und m wie oben, dann ist

$$\psi_{im}(a)\psi_{i'm}(a'^{-1}) = \psi_{im}(a)\psi_{i'm}(a')^{-1} =$$

$$= \psi_{im}(a)\psi_{im}(a)^{-1} = e_{G_m}.$$

Die Assoziativität bzw. Kommutativität von A folgen aus der Assoziativität bzw. Kommutativität der einzelnen A_i. A wird durch die folgende Zuordnung zu einer G-Gruppe

$$. \; G \times A \to A, \; ((s_i)_{i\in I}, \overline{a}) \longmapsto \overline{s_k(a)}, \;\; a \in A_k$$

Daß hierdurch eine Abbildung wohldefiniert ist, erkennt man wie folgt. Sind a, a' und m wie oben, dann gilt wegen $\varphi_{im}(s_m) = s_i$, $\varphi_{i'm}(s_m) = s_{i'}$:

$$\psi_{im}(s_i(a)) = \psi_{im}(\varphi_{im}(s_m)(a)) = s_m(\psi_{im}(a)) = s_m(\psi_{i'm}(a')) =$$

$$= \psi_{i'm}(\varphi_{i'm}(s_m)(a')) = \psi_{i'm}(s_{i'}(a')).$$

Außerdem gilt für $(s_i)_{i\in I,(t_i)_{i\in I}} \in G$; $a \in A_k$, $b \in A_j$ und $m \in I$ mit $k \leq m$, $j \leq m:$

(i) $e_G(\overline{a}) = \overline{e_{G_k}(a)} = \overline{a}$

(ii) $((s_i)_{i\in I}(t_i)_{i\in I})(\overline{a}) =$

$$= (s_i t_i)_{i\in I}(\overline{a}) = \overline{(s_k t_k)(a)} =$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$$= \overline{s_k(t_k(a))} = (s_i)_{i\in I}((t_i)_{i\in I}(\overline{a}))$$

(iii) $(s_i)_{i\in I}(\overline{a}\overline{b}) = (s_i)_{i\in I}\overline{(\psi_{km}(a)\psi_{jm}(b))} =$

$$= \overline{s_m(\psi_{km}(a)\psi_{jm}(b))} =$$

$$= \overline{s_m(\psi_{km}(a))s_m(\psi_{jm}(b))} =$$

$$= \overline{s_m(\psi_{km}(a))s_m(\psi_{jm}(b))} =$$

$$= (s_i)_{i\in I}(\overline{a})(s_i)_{i\in I}(\overline{b}).$$

G operiert also auf A. Diese Operation ist stetig, denn für jedes $a \in A_k$ ist

$G_a = \{(s_i)_{i\in I} \in G : (s_i)_{i\in I}(\overline{a}) = \overline{a}\} =$

= Urbild von $G_{k,a}$ unter der Projektionsabbildung $p_k : G \to G_k$

Da p_k stetig und $G_{k,a}$ offen ist, ist auch G_a offen. Bezüglich der diskreten Topologie ist A also eine diskrete G-Gruppe, vgl. (8.1). Damit ist der Beweis von (8.3) beendet.

Sei G eine proendliche Gruppe und sei $\mathcal{N}$ die Menge aller offenen Normalteiler von G. Sei A eine diskrete G-Menge bzw. diskrete G-Gruppe. Dann ist $(\mathcal{N}, G/N, f_{M,N})$, mit $f_{M,N}$ =Projektionsabbildung $G/N \to G/M$ für $M, N \in \mathcal{N}$ mit $N \subset M$, ein projektives System mit $G = \varprojlim G/N$, und $(\mathcal{N}, A^N, g_{M,N})$, mit $g_{M,N}$ =Inklusionsabbildung $A^M \hookrightarrow A^N$ für $M, N \in \mathcal{N}$ mit $N \subset M$, ein induktives System mit $A = \varinjlim A^N$. Die A^N, $N \in \mathcal{N}$, sind G/N-Mengen bzw. G/N-Gruppen. Also gilt

(8.4) **Satz** *Jede diskrete G-Menge bzw. G-Gruppe ist direkter Grenzwert von G_i-Mengen bzw. G_i-Gruppen mit endlichen Gruppen G_i*

Definition Sei G eine proendliche Gruppe, sei $\mathcal{N}$ die Menge aller offenen Normalteiler von G und sei A eine diskrete G-Gruppe. Dann ist für $q \in \{0, 1\}$, und wenn A ein diskreter G-Modul ist auch für $q = 2$, durch

$$(\mathcal{N}, H^q(G/N, A^N), \inf{}^{G/N}_{G/M})_{N\subset M} ,$$

ein induktives System von punktierten Kohomologiemengen bzw. von Kohomologiegruppen definiert; dabei ist für $M, N \in \mathcal{N}$ mit $N \subset M$

$$\inf{}^{G/N}_{G/M} : H^q(G/M, A^M) \to H^q(G/N, A^N)$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

die durch die Projektionsabbildung $f_{M,N} : G/N \to G/M$ induzierte Inflationsabbildung. Es sei

(8.5) $H^q(G, A) := \varinjlim_{N \in \mathcal{N}} H^q(G/N, A^N)$

der entsprechende induktive Grenzwert. Im Fall $q = 1$ oder $q = 2$ existiert zu jedem stetigen Kozykel $\alpha : G^q \to A$ ein offener Normalteiler $N \trianglelefteq G$ und ein Kozykel $\beta : (G/N)^q \to A^N$, so daß für die entsprechenden Kozykelklassen $(\alpha) \in H^q(G, A)$ und $(\beta) \in H^q(G/N, A^N)$ gilt

(8.6) $(\alpha) = \inf^G_{G/N}((\beta))$.

Viele der bisherigen Ergebnisse zur Kohomologie endlicher Gruppen und endlicher Galoisgruppen lassen sich mit Hilfe von (8.5) und (8.6) auf proendliche Gruppen und proendliche Galoisgruppen übertragen, insbesondere die in §4 erwähnte exakte Hochschild-Serre Sequenz; vgl. z.B. [SH], Chapter II..

(8.7) **Beispiele** (a) (vgl. z.B. [$SE2$], Chapter II, §1, 1.2) Sei k ein Körper und sei n eine natürliche Zahl, die zur Charakteristik von k teilerfremd ist. Sei $\overline{k}$ ein separabler algebraischer Abschluß von k und μ_n die Gruppe aller n-ten Einheitswurzeln in $\overline{k}$. Bezeichnet $(\ )^n : \overline{k}^* \to \overline{k}^*$ die Abbildung $x \mapsto x^n$, dann erhält man die folgende exakte Sequenz von G_k-Gruppen, wobei $G_k = G(\overline{k}/k)$:

$$1 \to \mu_n \to \overline{k}^* \xrightarrow{(\ )^n} \overline{k}^* \to 1.$$

Wegen $H^0(G_k, \overline{k}^*) = k^*$ und $H^1(G_k, \overline{k}^*) = 1$ (vgl. (1.7)) erhält man aus dieser exakten Sequenz mit Hilfe der proendlichen Version von (4.6) die folgende exakte Sequenz

$$k^* \xrightarrow{(\ )^n} k^* \xrightarrow{\delta} H^1(G_k, \mu_n) \to 1.$$

Also induziert δ einen Isomorphismus

$$\widetilde{\delta} : k^*/k^{*n} \cong H^1(G_k, \mu_n).$$

Dieser Isomorphismus läßt sich explizit wie folgt angeben: Für $a \in k^*$ sei $b \in \overline{k}^*$ so, daß $b^n = a$. Dann ist

$$\widetilde{\delta}(a \bmod k^{*n}) := (\alpha) \in H^1(G_k, \mu_n),$$

wobei

$$\alpha(s) = s(b)/b,\ s \in G_k.$$

Sei $P \subset \overline{k}$ die Menge aller Nullstellen eines irreduziblen Polynoms der Form $t^n - a \in k[t]$ und sei $L \subset \overline{k}$ der Körper, der aus k durch Adjunktion aller

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Elemente aus P entsteht. L ist eine endliche Galoiserweiterung von k, und die Einschränkung von α auf $G_L := G(\overline{k}/L)$ ist kohomologisch trivial. Somit ist (α) aufgrund der exakten Sequenz

$$1 \to H^1(G(L/k), \mu_n) \overset{\inf}{\to} H^1(G_k, \mu_n) \overset{res}{\to} H^1(G_L, \mu_n)$$

von der Form

$$(\alpha) = \inf_{G(L/k)}^{G_k}((\beta))$$

mit einem durch (α) eindeutig bestimmten Element $(\beta) \in H^1(G(L/k), \mu_n)$. P ist eine Links-$G(L/k)$-Menge, auf der μ_n so durch Multiplikation operiert, daß P ein prinzipaler homogener Raum für μ_n wird, dessen Aequivalenzklasse durch (β) und damit durch (α) eindeutig bestimmt ist. Unter der Annahme $\mu_n \leq k^*$ ist $H^1(G_k, \mu_n) = Hom(G_k, \mu_n)$, so daß in diesem Fall

$$\widetilde{\delta} : k^*/k^{*n} \cong Hom(G_k, \mu_n).$$

Die Elemente aus $Hom(G_k, \mu_n)$, also die stetigen Homomorphismen $\chi : G_k \to \mu_n$, entsprechen nach dem Hauptsatz der Galoistheorie (7.6) unter der folgenden Zuordnung bijektiv den cyclischen Körpererweiterungen von k in $\overline{k}$, deren Grad ein Teiler von n ist:

$$\chi \mapsto k_\chi := \overline{k}^{Kern(\chi)} = \text{Fixkörper von } \overline{k} \text{ unter der offenen Untergruppe } Kern(\chi) \text{ von } G_k.$$

(b) (vgl. [$SE5$], §1, 1.3; [BK], Chapter V, §6) Eine *étale Algebra* E von endlichem Rang über einem Körper k mit dem separablen algebraischen Abschluß $\overline{k}$ von k ist ein endliches Produkt von separablen Körpererweiterungen K_i von k mit $K_i \subset \overline{k}$. Die k-Isomorphieklassen solcher Algebren vom Rang n über k entsprechen bijektiv den Elementen der Kohomologiemenge $H^1(G_k, S_n)$, wobei die Galoisgruppe $G_k = G(\overline{k}/k)$ trivial auf der symmetrischen Gruppe S_n vom Grad n operiert. Diese Korrespondenz ist wie folgt: Sei E eine etale k-Algebra vom Rang n und $F(E)$ die Menge der n k-Algebra Homomorphismen $\varphi : E \to \overline{k}$. G_k operiert in natürlicher Weise auf $F(E)$. Identifiziert man $F(E)$ mit $\{1, ..., n\}$, so erhält man durch diese Operation einen Homomorphismus $f_E : G_k \to S_n$. Ist $\kappa : E \to E'$ ein k-Isomorphismus, dann ist $f_{E'}(s) = \sigma_\kappa f_E(s)\sigma_\kappa^{-1}$ für alle $s \in G_k$, wobei σ_κ der durch κ induzierten Bijektion $M(E) \to M(E')$ entspricht. Ist umgekehrt $(\alpha) \in H^1(G_k, S_n)$ die Klasse eines Homomorphismus $\alpha : G_k \to S_n$, dann sei E die Twistung der etalen k-Algebra $k \times ... \times k$ (n mal) mit α im Sinne von § 3. Das Bild von α ist isomorph zur Galoisgruppe der kleinsten Galoiserweiterung K von k, so daß $E \otimes_k K$ zerfällt, d.h. isomorph zu $K \times ... \times K$ (n mal) ist.

Definition (vgl. [$SE2$], Chapter II, §1, 1.1) Sei k ein Körper, sei $\overline{k}$ ein separabler algebraischer Abschluß von k und sei $K \longmapsto A(K)$ ein Funktor von

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

der Kategorie der separablen algebraischen Kópererweiterungen $K/k \subset \overline{k}/k$ in die Kategorie der diskreten Gruppen, so daß die folgenden Bedingungen erfüllt sind:

(1) $A(K) = \varinjlim A(K_i)$

wobei K_i, $i \in I$, die Menge aller Teilerweiterungen von K/k endlichen Grades durchläuft und der induktive Grenzwert der des induktiven Systems $(I, A(K_i), f_{ij})$ mit den durch die Inklusionen $K_i \subset K_j$ induzierten Homomorphismen $f_{ij} : A(K_i) \to A(K_j)$ ist

(2) Ist $K \subset K' \subset \overline{k}$, dann ist der induzierte Homomorphismus $A(K) \to A(K')$ injektiv

(3) Ist K'/K eine Galoiserweiterung mit $K' \subset \overline{k}$, dann operiert die Galoisgruppe $G = G(K'/K)$ auf $A(K')$, und es gilt

$A(K) = A(K')^G$

Dann heißt A ein *galoisscher Gruppenfunktor über* k.

(8.8) **Bemerkung** Ist A ein galoisscher Gruppenfunktor über k, dann gilt für jede Galoiserweiterung $K/k \subset \overline{k}/k$ und jedes $q \in \{0, 1, 2\}$, wobei A für $q = 2$ als kommutativ vorausgesetzt wird,

$H^q(G(K/k), A(K)) = \varinjlim H^q(G(K_i/k), A(K_i))$;

dabei durchläuft $K_i/k, i \in I$, alle endlichen Galoiserweiterungen von K/k, und der induktive Grenzwert ist der des induktiven Systems

$(I, H^q(G(K_i/k), A(K_i)), g_{ij})$

mit den durch die Inklusionen $K_i \subset K_j$ induzierten Inflationsabbildungen

$g_{ij} := \inf_{K_i}^{K_j} : H^q(G(K_i/k), A(K_i)) \to H^q(G(K_j/k), A(K_j))$

Definition Sei $\mathfrak{G}(k)$ die Kategorie der separablen algebraischen Körpererweiterungen $K/k \subset \overline{k}/k$. Eine Galoiskategorie $\mathfrak{F}$ über $\mathfrak{G}(k)$ heißt *zulässig*, wenn für jedes proendliche k-Objekt X von $\mathfrak{F}$ durch die Zuordnung $K \mapsto A_K := Aut(X_K)$, $(K \subset K') \mapsto (A(K) \to A(K'))$, ein galoisscher Gruppenfunktor von $\mathfrak{G}(k)$ in die Kategorie der diskreten Gruppen über k definiert wird.

Wir sind nun in der Lage, mit Hilfe von (5.2), (e) die in (1.7) und (2.1) gegebene kohomologische Beschreibung von k-Isomorphieklassen getwisteter Objekte in Galoiskategorien in der folgenden Weise auf unendliche Galoiserweiterungen zu übertragen.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

(8.9) **Satz** *Sei k ein Körper, sei $\overline{k}$ ein separabler algebraischer Abschluß von k und sei $G_k = G(\overline{k}/k)$ die Galoisgruppe von $\overline{k}/k$. Sei weiterhin $\mathfrak{G}(k)$ die Kategorie der separablen algebraischen Körpererweiterung von k in $\overline{k}$ und sei $\mathfrak{F}$ eine zulässige Galoiskategorie über $\mathfrak{G}(k)$. Dann ist für jedes proendliche k-Objekt X von $\mathfrak{F}$ die Abbildung*

$$E_{\mathfrak{F}}(\overline{k}/k, X) \xrightarrow{\theta} H^1(G_k, Aut(X_{\overline{k}}))$$

$$\theta((Y)) := (s \mapsto f^{-1} \circ f^s), \;\; f \in Isom(X_{\overline{k}}, Y_{\overline{k}}),$$

von der Menge aller k-Isomorphieklassen von $\overline{k}/k$-Twistungen von X in die 1-te Kohomologiemenge der proendlichen Gruppe G_k bezüglich der Automorphismengruppe von $X_{\overline{k}}$ injektiv und bildet das ausgezeichnete Element auf die Klasse des trivialen 1-Kozykels ab. Für den Fall, daß $\mathfrak{F}$ eine der in § 2 definierten speziellen Kategorien $\mathfrak{T}_{p,q}$ oder die spezielle Galoiskategorie der quadratischen Räume ist, ist θ bijektiv.

Definition Sei A ein galoisscher Gruppenfunktor über k und sei $q \in \{0, 1, 2\}$. Ein Zwischenkörper K von $\overline{k}/k$ heißt *Zerfällungskörper von* $(\alpha) \in H^q(G_k, A(\overline{k}))$, wobei A im Fall $q = 2$ als kommutativ vorausgesetzt wird, wenn (α) im Kern der Restriktionsabbildung $res_k^K : H^q(G_k, A(\overline{k})) \to H^q(G(\overline{k}/K), A(\overline{k}))$ enthalten ist.

Aufgaben und Beispiele

(1) Verifizieren Sie alle in den Beispielen (8.7), (a) und (b), gemachten Behauptungen.

(2) Bestimmen Sie in den Beispielen (8.7),(a) und (b), jeweils einen Zerfällungskörper für die entsprechenden 1-Kozykelklassen. (Ziemlich leicht)

(3) Beweisen Sie eine proendliche Version der Aussage in Aufgabe 4 zu §5 und geben Sie für den Fall, daß $\mathcal{G} = G(\overline{k}/k)$ die Galoisgruppe eines separabel algebraisch abgeschlossenen Oberkörpers $\overline{k}$ des Körpers k ist, eine Interpretation dieser Aussage im Rahmen des körpertheoretischen Einbettungsproblems. (Vgl. $[HM]$, insbesondere Abschnitte 1 und 2)

§ 9. Die kohomologische Beschreibung der Brauergruppe eines Körpers

In diesem Abschnitt besprechen wir eine kohomologische Beschreibung für die Brauergruppe eines Körpers und übernehmen dabei weitgehend die entsprechende Darstellung in $[SE1]$, Chapter X, §4, §5, §7.

Sei k ein Körper und sei C eine endlichdimensionale assoziative k-Algebra. Die Theorie von Wedderburn, die beispielsweise in $[D]$ und $[KT]$ dargestellt wird, beinhaltet den folgenden Satz.

(9.1) **Satz** *Die folgenden Aussagen sind aequivalent*

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

(a) *C hat kein nichttriviales 2-seitiges Ideal, und das Zentrum von C ist k.*

(b) *Ist κ ein algebraischer Abschluß von k, dann ist $C \otimes_k \kappa$ als κ-Algebra isomorph zu einer Matrixalgebra über κ.*

(c) *Es existiert eine endliche Galoiserweiterung $K/k \subset \kappa/k$, so daß $C \otimes_k K$ als K-Algebra isomorph zu einer Matrixalgebra über K ist.*

(d) *Es gibt einen durch C bis auf k-Isomorphie eindeutig bestimmten Schiefkörper D mit dem Zentrum k und eine durch C eindeutig bestimmte natürliche Zahl n, so daß C als k-Algebra isomorph zur Matrixalgebra $Mat(n \times n, D)$ ist.*

Definition Eine endlichdimensionale, assoziative k-Algebra, die eine der aequivalenten Eigenschaften des vorstehenden Satzes besitzt, heißt *zentraleinfache k-Algebra*. Ist C eine zentraleinfache k-Algebra und K/k eine Körpererweiterung, so daß $C \otimes_k K$ eine Matrixalgebra über K ist, dann heißt K ein *Zerfällungskörper* von C.

(9.2) **Beispiele** Die folgenden Beispiele werden in vielen Büchern über Brauergruppen erklärt. Wir begnügen uns hier, abgesehen von Beispiel (c), mit einer kurzen Auflistung.

(a) Jede Matrixalgebra $Mat(n \times n, k)$ ist zentraleinfach.

(b) Für $k = \mathbb{R}$ wird auf dem 4-dimensionalen $\mathbb{R}$-Vektorraum mit Baiselementen $1, i, j, k$, also auf

$$\mathbb{H} := \mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$

durch

$$1 \cdot h = h,\ ah = ha \text{ für alle } h \in \mathbb{H},\ a \in \mathbb{R}$$
$$i^2 = j^2 = k^2 = -1$$
$$ij = -ji = k,\ jk = -kj = i, ki = -ik = j$$

eine Multiplikation definiert, bezüglich der $\mathbb{H}$ zu einem Schiefkörper mit dem Zentrum $\mathbb{R}$ wird; insbesondere ist $\mathbb{H}$ eine zentraleinfache $\mathbb{R}$-Algebra mit dem Zerfällungskörper $\mathbb{C}$. $\mathbb{H}$ heißt der Schiefkörper der Hamilton Quaternionen. $\mathbb{H}$ läßt sich als $\mathbb{R}$-Algebra erzeugen durch i und j und ist als solche vollständig bestimmt durch die Relationen

$$ij = -ji,\ \ i^2 = -1,\ \ j^2 = -1.$$

(c) Sei m eine natürliche Zahl und sei k im Körper, der eine primitive m-te Einheitswurzel ξ enthält.Seien außerdem $a, b \in k^*$. Sei $A_\xi(a, b)$ die assoziative k-Algebra mit Einselement 1, die über k erzeugt wird durch zwei Elemente x, y, so daß die folgenden Relationen erfüllt sind

$$yx = \xi xy,\ \ x^m = a1,\ y^m = b1;$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

die Monome $x^i y^j$, $0 \leq i < m$, $0 \leq j < m$, bilden also eine k-Vektorraum Basis von $A_\xi(a,b)$. Die Bedingungen für eine assoziative Algebra mit Einselement lassen sich für $A_\xi(a,b)$ durch direktes Nachrechnen leicht bestätigen. $A = A_\xi(a,b)$ ist außerdem zentraleinfach über k. Um das einzusehen, wiederholen wir die entsprechende Argumentation in [$MN1$], §7, p.144 ff, und betrachten die k-linearen Abbildungen

$$T_x : A \to A,\ a \mapsto xax^{-1};\ T_y : A \to A,\ a \mapsto yay^{-1}.$$

Jeder Basisvektor der Form $x^i y^y$ ist ein Eigenvektor sowohl von T_x als auch von T_y mit Eigenwerten ξ^{-j} bzw. ξ^i. Das Zentrum von A ist somit $kx^0y^0 = k1 = k$. A ist einfach: Sei dazu $\mathfrak{b} \subset A$ ein zweiseitiges Ideal und sei $b_0 \in \mathfrak{b}$, $b_0 \neq 0$. Wir schreiben

$$b_0 = \sum_{i,j=0}^{m-1} \beta_{ij} \cdot x^i y^j \quad \text{mit Koeffizienten} \quad \beta_{ij} \in k.$$

Mindestens einer der Koeffizienten β_{ij} ist $\neq 0$, etwa $\beta_{\gamma q} \neq 0$. Sei

$$b_1 := x^{-p} b_0 y^{-q}\ .$$

Dann ist b_1 Element von $\mathfrak{b}$ und hat die Form

$$b_1 = \sum_{i,j=0}^{m-1} \gamma_{ij} \cdot x^i y^j \ \text{mit}\ \gamma_{00} \neq 0.$$

Sei

$$b_2 := (T_x - \xi)(T_x - \xi^2)...(T_x - \xi^{m-1})b_1.$$

Dann ist b_2 Element von $\mathfrak{b}$ und hat die Form

$$b_2 = (1-\xi)(1-\xi^2)...(1-\xi^{m-1}) \sum_{i=0}^{m-1} \gamma_{i0} x^i.$$

Ähnlich erkennt man, daß

$$b_3 := (T_y - \xi)(T_y - \xi^2)...(T_y - \xi^{m-1})b_2$$

Element von $\mathfrak{b}$ ist und die Form

$$b_3 = (1-\xi)^2(1-\xi^2)^2...(1-\xi^{m-1})^2\gamma_{00} \cdot 1$$

hat. Insbesondere ist b_3 eine Einheit in $\mathfrak{b}$, also gilt $\mathfrak{b} = A$.

$A_\xi(a,b)$ heißt auch die durch ξ, a und b definierte *Symbolalgebra* und im Fall $\xi = -1$ die durch a und b definierte *verallgemeinerte Quaternionenalgebra*. Für eine andere Einführung von Symbolalgebren vgl. [$SE1$], Chapter XIV, §2.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Zwei zentraleinfache k-Algebren heißen aequivalent, wenn die nach (9.1), (d), zu diesen Algebren gehörigen Schiefkörper als k-Algebren isomorph sind. Hierdurch wird eine Aequivalenzrelation definiert. Sei

$$Br(k) := \{(C) : C \text{ zentraleinfache } k\text{-Algebra}\}$$

die Menge der entsprechenden Aequivalenzklassen. Das Tensorprodukt von k-Algebren induziert auf $Br(k)$ eine kommutative Gruppenstruktur mit dem neutralen Element (k); das zu $(C) \in Br(k)$ inverse Element ist gegeben durch $(C)^{-1} := (C^0)$, wobei C^0 die zu C entgegengesetzte Algebra ist, d.h. $C^0 = C$ als k-Vektorraum, und für alle $x, y \in C$ ist xy in C^0 gleich xy in C; vgl. dazu $[D]$, IV, §4, insbesondere Satz 11.

Definition $Br(k)$ mit dieser Multiplikation heißt die *Brauergruppe von k*.

Ist K/k eine Körpererweiterung, dann ist die durch das Tensorprodukt mit K induzierte Abbildung

$$Br(k) \to Br(K),\ (C) \mapsto (C \otimes_k K)$$

ein Homomorphismus von abelschen Gruppen. Sei $Br(K/k)$ der Kern dieses Homomorphismus. Der obige Satz (9.1), Teil (c), zeigt, daß

$$Br(k) = \cup_{K/k} Br(K/k),$$

wobei K/k alle endlichen Galoiserweiterungen durchläuft. Sei K/k eine endliche Galoiserweiterung und sei $Br(n, K/k)$ die Menge aller Aequivalenzklassen zentraleinfacher k-Algebren C mit

$$C \otimes_k K \cong Mat(n \times n, K)$$

Es gilt

$$Br(K/k) = \cup_{n\in\mathbb{N}} Br(n, K/k).$$

Wie in Beispiel (2.2), (c), erklärt wurde, ist durch jede zentraleinfache k-Algebra C ein tensorielles k-Objekt $((V, \delta), x)$ vom Typ $(1, 2)$ definiert; dabei ist V der k-Vektorraum C, $\delta : V \to V^*$ ein k-Isomorphismus von V mit seinem Dualraum und $x \in V \otimes V^* \otimes V^*$ ein Tensor vom Typ $(1, 2)$, der der k-bilinearen Ringmultiplikation $\alpha : V \times V \to V$ entspricht. Aufgrund von (9.1) ist also mit den Bezeichnungen von (2.2), (c):

$$E_{\mathfrak{T}_{1,2}}(K/k, ((V, \delta), x)) = E(K/k, (V, \alpha)) = Br(n, K/k).$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Um die Gruppe aller K-Automorphismen von $(V,\alpha)_K$ beschreiben zu können, machen wir Gebrauch von dem sogenannten Satz von Skolem-Noether, vgl. [D], IV, §4, insbesondere Satz 3.

(9.3) **Satz** *Jeder k-Automorphismus t einer zentraleinfachen k-Algebra B ist ein innerer Automorphismus, d.h. es existiert eine Einheit $u \in B^*$, so daß $t(x) = uxu^{-1}$ für alle $x \in B$.*

Dieser Satz impliziert, daß die Gruppe aller k-Automorphismen einer Matrixalgebra $B = Mat(n \times n, k)$ isomorph zur projektiven linearen Gruppe $PGL(n,k) \cong GL(n,k)/k^*$ ist. Angewandt auf die vorliegende Situation einer zentraleinfachen k-Algebra C mit der Eigenschaft $(C) \in Br(n, K/k)$ ist also die Gruppe aller K-Automorphismen $A_K(V,\alpha) = Aut(V \otimes K, \alpha \otimes K)$ des zugehörigen Paars (V,α) isomorph zur projektiven linearen Gruppe vom Grad n über K:

$$A_K(V,\alpha) \cong PGL(n,K);$$

und wenn K/k eine endliche Galoiserweiterung mit der Galoisgruppe G ist, dann ist dieser Isomorphismus G-verträglich. Die in (2.1) konstruierte Bijektion

$$\theta : E(K/k,(V,\alpha)) \to H^1(G, A_K(V,\alpha))$$

wird somit zu einer Bijektion.

$$(9.4) \quad \theta_n : Br(n, K/k) \to H^1(G, PGL(n,K)),$$

die wie folgt aussieht: Jeder Klasse $(C) \in Br(n, K/k)$ wird die Klasse des 1-Kozykels

$$G \to PGL(n,K),\ s \mapsto s(f) \circ f^{-1},$$

wobei

$$f : C \otimes_k K \to Mat(n \times n, K)$$

ein Isomorphismus von K-Algebren ist, zugeordnet. Die exakte Sequenz von G-Gruppen

$$1 \to K^* \to GL(n,K) \xrightarrow{\pi} PGL(n,K) \to 1$$

definiert aufgrund der allgemeinen Konstruktion in § 4 eine Korandabbildung

$$\Delta_n : H^1(G, PGL(n,K)) \to H^2(G, K^*),$$

die hier so aussieht: Jeder Klasse von 1-Kozykeln $(P) \in H^1(G, PGL(n,K))$ wird die Klasse des 2-Kozykels

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$\alpha : G \times G \to K^*$

mit

$T(s)s(T(t)) = \alpha(s,t)T(st),\ s,t \in G,$

zugeordnet; dabei ist

$T : G \to GL(n,K)$

ein Schnitt zu P, d.h. eine Abbildung mit der Eigenschaft

$P = \pi \circ T : G \xrightarrow{T} GL(n,K) \xrightarrow{\pi} PGL(n,K).$

Durch Hintereinanderausführung der Abbildungen θ_n und Δ_n erhält man eine Abbildung

$\delta_n : Br(n,K/k) \to H^2(G,K^*).$

Einfache Eigenschaften des Tensorprodukts von Algebren zeigen, daß für alle $n,n' \in \mathbb{N}$ und alle $(C) \in Br(n,K/k)$, $(C') \in Br(n',K/k)$ die folgende Formel gilt:

$\delta_{nn'}((C \otimes_k C')) = \delta_n((C))\delta_{n'}((C')).$

Somit erhält man einen Homomorphismus

$\delta = \delta_{K/k} : Br(K/k) \to H^2(K/k) := H^2(G,K^*).$

(9.5) **Satz** *Der Homomorphismus δ ist bijektiv.*

Beweis: Wir erinnern an die Ausführungen in Beispiel (4.7), (b): Die Injektivität von δ ergibt sich wegen (9.4) aus $H^1(G,GL(n,K)) = \{1\}$ und der daraus resultierenden Trivialität des Kerns der Abbildung Δ_n. Um die Surjektivität von δ zu zeigen, reicht es, die Surjektivität der Abbildung δ_n für $n = (K : k)$ zu beweisen. Letzteres wiederum ergibt sich wegen (9.4) aus der Surjektivität der Abbildung Δ_n, welche in (4.7), (b), nachgewiesen wurde. Damit ist der Beweis von (9.5) beendet.

Sei K'/k eine endliche Galoiserweiterung, die die Galoiserweiterung K/k enthält. Man erhält eine Einbettung

$Br(K/k) \xrightarrow{\iota_K^{K'}} Br(K'/k),$

und das folgende Diagramm ist kommutativ

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$$
\begin{array}{ccc}
Br(K'/k) & \overset{\delta_{K'/k}}{\rightarrow} & H^2(K'/k) \\
\iota_K^{K'} \uparrow & & \uparrow inf_K^{K'} \\
Br(K/k) & \overset{\delta_{K/k}}{\rightarrow} & H^2(K/k).
\end{array}
$$

Daraus ergibt sich, daß die induktiven Grenzwerte der entsprechenden induktiven Systeme

$$(I, Br(K_i/k), \iota_{ij}), \quad (I, H^2(K_i/k), inf_{K_i}^{K_j}),$$

wobei $\{K_i : i \in I\}$ die Menge aller endlichen Galoiserweiterungen von k in einem separabel algebraischen Abschluß $\overline{k}$ von k bezeichnet, isomorph sind. Ist $\overline{k}$ ein separabel algebraischer Abschluß von k und $G_k = G(\overline{k}/k)$ die Galoisgruppe von $\overline{k}$ über k, so ergibt sich also mit Hilfe von (8.9) der folgende Satz.

(9.6) **Satz** *Die Brauergruppe von k ist isomorph zur 2-ten Kohomologiegruppe von G_k bezüglich $\overline{k}^*$:*

$$Br(k) \cong H^2(G_k, \overline{k}^*).$$

Diese kohomologische Beschreibung der Brauergruppe zeigt insbesondere, daß ein Zwischenkörper K von $\overline{k}/k$ genau dann ein Zerfällungskörper einer zentraleinfachen k-Algebra A ist, wenn K ein Zerfällungskörper des (A) entsprechenden Elementes in $H^2(G_k, \overline{k}^*)$ im Sinne der Definition aus §8 ist.

(9.7) **Beispiele** Die nachfolgenden Beispiele sind wohlbekannt; vgl. $[SE1]$, Chapter X, §7, und die dort gemachten Literaturangaben.

(a) Sei k ein endlicher Körper und sei K/k eine endliche Galoiserweiterung mit der Galoisgruppe G. Bekanntlich ist G cyclisch, so daß also nach §4, Aufgaben und Beispiele (9)

$$H^2(G, K^*) \cong k^*/Norm_{K/k}(K^*).$$

Der letzte Term ist trivial, weil die Normabbildung

$$N = Norm_{K/k} : K^* \to k^*$$

surjektiv ist. Somit ist die Brauergruppe $Br(k)$ trivial. Daraus ergibt sich auch das wohlbekannte Resultat von Wedderburn, demzufolge jeder endliche Schiefkörper kommutativ ist.

(Die Surjektivität der Normabbildung

$$N : K^* \to k^*,\ \alpha \mapsto \alpha\alpha^q ... \alpha^{q^{n-1}} = \alpha^{(q^n-1)/(q-1)},$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$n = (K : k)$, $q = |k|$, ergibt sich aus

$|Kern(N)| = \frac{q^n-1}{q-1}$;

denn

$|Bild(N)| = |K^*| \,/\, |Kern(N)| = (\frac{q^n-1}{q^n-1})(q-1) = q-1 = |k^*|\,.)$

(b) Sei $k = \mathbb{R}$. Dann gilt

$$Br(k) \cong H^2(G(\mathbb{C}/\mathbb{R}), \mathbb{C}^*) \cong \widehat{H}^0(G(\mathbb{C}/\ \mathbb{R}), \mathbb{C}^*) \cong \mathbb{R}^*/\mathbb{R}^*_{>0} \cong \mathbb{Z}/2\mathbb{Z}$$

wobei $\mathbb{R}^*_{>0}$ die multiplikative Gruppe aller reellen Zahlen > 0 bezeichnet. Das nichttriviale Element in $Br(\mathbb{R})$ wird repräsentiert durch die Quotientenalgebra $\mathbb{H}$.

(c) Sei k ein Körper, der vollständig bezüglich einer diskreten Bewertung v ist und dessen Restklassenkörper $\widetilde{k}$ vollkommen ist. Dann erhält man durch Auswahl eines Primelementes für v eine zerfallende exakte Sequenz

$$1 \to Br(\widetilde{k}) \to Br(k) \to Hom(G_{\widetilde{k}}, \mathbb{Q}/\mathbb{Z}) \to 0,$$

vgl. $[WT2]$; $[SE1]$, Chapter XII. Ist $\widetilde{k}$ endlich, dann existiert ein Isomorphismus

$$inv_k : Br(k) \overset{\cong}{\to} \mathbb{Q}/\mathbb{Z}$$

mit der folgenden Eigenschaft: Ist $k'/k \subset \overline{k}/k$ eine Erweiterung vom Grad $n = (k' : k)$ und ist $Res_{k'k} : Br(k) \to Br(k')$ der durch $(A) \mapsto (A \otimes_k k')$ induzierte Homomorphismus, dann gilt

$$inv_{k'} \circ Res_{k'/k} = n \cdot inv_k\ ,$$

vgl. $[SE1]$, Chapter XIII..

(d) Sei k ein Zahlkörper, d.h.eine endliche Erweiterung von $\mathbb{Q}$, und seien $\{k_v\}_v$ seine Komplettierungen bezüglich aller Bewertungen v von k. Dann ist die folgende Sequenz exakt

$$1 \to Br(k) \to \oplus_v Br(k_v) \overset{\Sigma_v inv_v}{\to} \mathbb{Q}/\mathbb{Z} \to 0,$$

vgl. $[D]$, VII, §5. Das ist der sogenannte Hauptsatz von Hasse-Brauer-Noether in der Theorie der zentraleinfachen Algebren über Zahlkörpern.

(e) (vgl. z.B. $[SE1]$, Chapter X, §7) Ein Körper k heißt quasialgebraisch abgeschlossen oder C_1-Körper, wenn für jedes homogene Polynom $f(X_1, ..., X_n)$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

vom Grad $d \neq 0$ in n Veränderlichen, das nur die triviale Nullstelle $(0, ..., 0) \in k^n$ besitzt, die Ungleichung $d \geq n$ erfüllt ist. Jeder algebraisch abgeschlossene Körper ist quasialgebraisch abgeschlossen. Die Brauergruppe jeder endlichen Erweiterung K/k eines jeden C_1-Körpers k ist trivial: Um das zu einzusehen betrachtet man einen Schiefkörper D mit dem Zentrum K. Es gilt $\dim_K(D) = r^2$. Sei $s := (K : k)$ der Grad von K über k. Für $x \in D$ sei $Nrd(x) \in K$ die reduzierte Norm von x (Ist L ein Zerfällungskörper von D und $\iota : D \otimes_K L \to Mat(r \times r, L)$ ein Isomorphismus, dann ist $Nrd(x) := \det(\iota(x \otimes 1))$, wobei $x \otimes 1 \in D \otimes_K L$ das Bild von $x \in D$ in $D \otimes_K L$ bezeichnet. Diese Definition von Nrd erweist sich als unabhängig von der Auswahl des Zerfällungskörpers L von D, vgl. [D], IV, §7.) Setze

$$f(x) := Norm_{K/k}(Nrd(x)),\ x \in D.$$

f verschwindet nur bei $x = 0$. Ist $e_1, ..., e_n$ eine Basis von D über k und schreibt man $x = \sum_{i=1}^n x_i e_i$, dann läßt sich f als Polynom in den $n = sr^2$ Veränderlichen $x_1, ..., x_n$ auffassen. f ist homogen vom Grad sr. Da k ein C_1-Körper ist, gilt $sr^2 \leq sr$, d.h. $r = 1$, und damit $D = K$. Da jede zentraleinfache K-Algebra isomorph zu einer Matrixalgebra über einem Schiefkörper mit Zentrum K ist, folgt

$$Br(K) = 1.$$

Beispiele von quasialgebraisch abgeschlossenen Körpern liefert der Satz von Tsen, vgl. z.B. [$LO2$], §27, oder [SH], Chapter IV, insbesondere §3.

Satz (Tsen) Ist k_0 ein algebraisch abgeschlossener Körper, dann ist der Körper $k_0(t)$ der rationalen Funktionen in nur einer Unbestimmten t über k_0 quasialgebraisch abgeschlossen.

(9.8) **Bemerkung** Sei k ein Körper und sei m eine zur Charakteristik von k teilerfremde natürliche Zahl. Sei $\overline{k}$ ein separabel algebraischer Abschluß von k und sei μ_m der G_k-Modul aller m-ten Einheitswurzeln in $\overline{k}$. Dann induziert die Einbettung $\mu_m \hookrightarrow \overline{k}^*$ einen Isomorphismus

$$H^2(G_k, \mu_m) \cong Br(k)_m,$$

wobei $Br(k)_m$ die Gruppe aller $(A) \in Br(k)$ mit $(A)^m = (k)$ bezeichnet.

Das folgt aus der zur exakten G_k-Sequenz

$$1 \to \mu_m \to \overline{k}^* \overset{(\,)^m}{\to} \overline{k}^* \to 1$$

gehörigen exakten Kohomologiesequenz

$$... \to H^1(G_k, \overline{k}^*) \overset{\delta}{\to} H^2(G_k, \mu_m) \to H^2(G_k, \overline{k}^*)_m \cong Br(k)_m$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

und der Trivialität von $H^1(G_k, \overline{k}^*)$, vgl. (1.8) in Verbindung mit (8.8).

(9.9) **Beispiel** Sei k ein Körper und sei m eine zur Charakteristik von k teilerfremde natürliche Zahl. Wir nehmen an, daß k eine primitive m-te Einheitswurzel ξ enthält. Seien außerdem $a, b \in k^*$ und $\alpha, \beta \in \overline{k}$ so, daß $\alpha^m = a$ und $\beta^m = b$. Wir definieren Homomorphismen

$$\lambda_a : G_k \to \mathbb{Z}/m\mathbb{Z}, \ \ \lambda_b : G_k \to \mathbb{Z}/m\mathbb{Z}$$

durch

$$s(a) =: \alpha\xi^{\lambda_a(s)}, \ s(b) =: \beta\xi^{\lambda_b(s)}, \ s \in G_k.$$

Mit Hilfe von λ_a und λ_b definieren wir die Abbildung

$$c : G_k \times G_k \to \mu_m, \ c(s,t) := \xi^{\lambda_a(s)\lambda_b(t)}, \ s, t \in G_k.$$

c ist ein 2-Kozykel. Deren Kohomologieklasse in $H^2(G_k, \mu_m)$ entspricht aufgrund von Bemerkung (9.8) ein Element in der Gruppe $Br(k)_m$; dieses Element wird durch die in Beispiel (9.2), (c), definierte verallgemeinerte Quaternionenalgebra $A_\xi(a, b)$ repräsentiert; vgl. dazu [$SE1$], Chapter XIV, §2, Proposition 5.

Ein bedeutendes Resultat von L.K. Merkurjev und A.K. Suslin [MS] besagt, daß die Gruppe $Br(k)_m$ von Klassen zentraleinfacher k-Algebren der Form $A_\xi(a, b)$, $a, b \in k^*$, erzeugt wird.

Für eine ausführliche Darstellung der Zusammenhänge zwischen zentraleinfachen Algebren und Galoiskohomologie vgl. auch [GS] und die dort genannte Literatur.

In [$G3$] wird die Brauergruppe eines Schemas definiert und untersucht; sie hat weitreichende Anwendungen in der algebraischen und arithmetischen Geometrie gefunden.

Aufgaben und Beispiele

(1) Erarbeiten Sie einen Beweis des Satzes von Tsen. (Vgl. z.B. [$LO2$], §27)

(2) Sei k ein Zahlkörper. Zeigen Sie, daß es zu jedem Element $(A) \in Br(k)$ eine natürliche Zahl m gibt, so daß $k(\mu_m)$ ein Zerfällungskörper von (A) ist. (Vgl. z.B. [D], VII, §5)

(3) Sei k ein Körper. Das Bild des Homomorphismus

$$H^2(G_k, k^*) \overset{k^* \hookrightarrow \overline{k}^*}{\to} H^2(G_k, \overline{k}^*) \cong Br(k)$$

heißt die *rationale Brauergruppe von k* und wird mit $Br(k)_{rat}$ bezeichnet. Ein Element $(\alpha) \in Br(k)$ heißt *zyklisch*, wenn eine zyklische Erweiterung $L/k \subset$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$\overline{k}/k$ existiert, so daß $(\alpha) \in Br(L/k)$. Sei $Br(k)_{cyc}$ die von allen zyklischen Elementen erzeugte Untergruppe von $Br(k)$.

Zeigen Sie, daß $Br(k)_{rat} = Br(k)_{cyc}$. (Die Begriffsbildung "Rationale Brauergruppe" und die wesentlichen Aussagen dieser Aufgabe stehen in [$LBVO$], part 1, 1.3, p. 13/14; sie werden dort einer Anregung von D. Saltman zugeschrieben. Verwenden Sie beim Beweis der Aussage $Br(k)_{rat} \subset Br(k)_{cyc}$ das gegen Ende dieses Paragraphen erwähnte Resultat von Merkurjev und Suslin; vgl. [$LBVO$], part 1, 1.3.9)

(4) Zeigen Sie: $Br(\mathbb{R}(t)) = \{(A_{-1}(-1, a)) : a \in \mathbb{R}(t)\}$. (Wohlbekannt; folgt aus (9.7), (b))

(5) Sei K/k eine endliche Galoiserweiterung mit der Galoisgruppe $G = G(K/k)$. Sei $(P) \in H^1(G, PGL(n, K))$. Dann teilt die Ordnung von $(f) = \Delta_n((P)) \in H^2(G, K^*)$ den "Grad" n von (P). Das kann man nach I. Schur [SCH], §1, Beweis von Satz I, wie fogt beweisen: Man wählt einen Schnitt $T : G \to GL(n, K)$ zu P mit $T(s)s(T(t)) = f(s, t)T(st)$ für alle $s, t \in G$ und bildet auf beiden Seiten der letzten Gleichung die Determinante.

(6) Sei k ein Körper und sei G_k die absolute Galoisgruppe von k. Wir nehmen an, daß G_k trivial auf der Gruppe $\mathbb{Q}/\mathbb{Z}$ operiert. Zeigen Sie jeweils unter Verwendung von Resultaten über die entsprechende Brauergruppe von k, daß $H^2(G_k, \mathbb{Q}/\mathbb{Z})$ in den folgenden Fällen trivial ist:

(a) $k = \mathbb{C}(t)$ ($H^2(G_k, \mathbb{Q}/\mathbb{Z})$ ist in diesem Fall isomorph zur Brauergruppe von k)

(b) $k = \mathbb{R}(t)$ ((a) anwenden)

(c) $k =$ endliche Erweiterung von $\mathbb{Q}_p$ (vgl. z.B. [$SE4$], §6)

(d) $k =$ endliche Erweiterung von $\mathbb{Q}$ (vgl. z.B. [$SE4$], §6)

§ 10. Quadratische Formen und die Brauergruppe

Die algebraische Theorie der quadratischen Formen über Korpern in ihrer heutigen Form wurde wesentlich durch die grundlegende Arbeit [$WT1$] von E. Witt geprägt. Eine umfassende Darstellung dieser Theorie ist in [$SC2$] enthalten. In diesem Abschnitt erläutern wir einen Zusammenhang zwischen quadratischen Formen über einem Körper mit von 2 verschiedener Charakteristik und der Brauergruppe dieses Körpers. Ein solcher Zusammenhang wird ebenfalls in [$WT1$] hergestellt, und in galoiskohomologischer Form in der grundlegenden Arbeit [SR]. Für eine Zusammenfassung der Wittschen Theorie und weitere Zusammenhänge zwischen quadratischen Formen und der Galoiskohomologie vgl. man auch [PF].

Wir folgen nachfolgend zunächst der Darstellung in [CH] und dann den Ausführungen in [$SE2$], III, §3, (3.2), Example b.

Sei k ein Körper mit $char(k) \neq 2$. Sei V ein endlichdimensionaler k-Vektorraum und sei $q : V \to k$ eine nichtausgeartete quadratische Form. Aus Beispiel (2.2), (b), wissen wir, daß für jede endliche Galoiserweiterung K/k mit der Galoisgruppe G die Menge $E(K/k, (V, q))$ aller k-Isomorphieklassen von nichtausgearteten quadratischen Räumen, die über K zu (V_K, q_K) isomorph sind, bijektiv zur Kohomologiemenge $H^1(G, O_K(q))$ ist, wobei $O_K(q)$ die orthogonale

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Gruppe von (V_K, q_K) ist. Und mit (8.9) erhalten wir durch Limesbildung die Bijektion

$$E(\overline{k}/k, (V,q)) \to H^1(G_k, O_{\overline{k}}(q)),$$

wobei $\overline{k}$ ein separabler algebraischer Abschluß von k ist. In diesem Abschnitt wollen wir nun versuchen, die Menge $H^1(G_k, O_{\overline{k}}(q))$ mit Hilfe der Brauergruppe besser zu vestehen. Dazu benötigen wir einige algebrentheoretische Konstruktionen, die wir zunächst erläutern, und übernehmen dabei weitgehend die entsprechende Darstellung in $[CH]$.

Definition Eine $\mathbb{Z}/2$-*Graduierung* einer endlichdimensionalen assoziativen k-Algebra A ist eine Darstellung von A als direkte Summe von k-Untervektorräumen A_0, A_1, also

$$A = A_0 \oplus A_1 \text{ als } k\text{-Vektorräume},$$

so daß gilt

$$\begin{aligned} &k \cdot 1_A \subset A_o \\ &A_0A_0 \subset A_0 \ , \ A_1A_1 \subset A_0 \\ &A_0A_1 \subset A_1 \ , \ A_1A_0 \subset A_1. \end{aligned}$$

A_0 ist also eine Teilalgebra von A. Die Untervektorräume A_i, $i = 0, 1$, heißen auch die homogenen Komponenten von Grad i, und A heißt auch $\mathbb{Z}/2$-*graduierte k-Algebra* mit der $\mathbb{Z}/2$-Graduierung (A_0, A_1).

Sei A eine $\mathbb{Z}/2$-graduierte k-Algebra mit homogenen Komponenten A_i, $i = 0, 1$. Die Abildung

$$\alpha : A \to A \text{ mit } \alpha_{|A_0} = id \text{ und } \alpha_{|A_1} = -id$$

ist ein k-Automorphismus von A mit der Eigenschaft $\alpha^2 = id$, der sogenannte *kanonische Automorphismus von A*. Ist umgekehrt $\alpha : A \to A$ ein k-Automorphismus mit der Eigenschaft $\alpha^2 = id$ und sind A_0 undA_1 die entsprechenden Eigenräume zu den Eigenwerten 1 bzw. -1 von α, dann definiert das Paar (A_0, A_1) eine $\mathbb{Z}/2$-Graduierung von A

(10.1) **Beispiele** (a) Jede endlichdimensionale, assoziative k-Algebra hat die sogenannte triviale Graduierung $A_0 = A$, $A_1 = \{0\}$.

(b) $A = K = k(\sqrt{d})$ sei eine quadratische Körpererweiterung. Dann gilt $A = A_0 \oplus A_1$ mit $A_0 = k \cdot 1 = k$, $A_1 = k \cdot \sqrt{d}$.

(c) Für $a, b \in k^*$ sei $A = A_{-1}(a, b)$ die zugehörige Quaternionenalgebra, d.h. A besitzt als k-Vektorraum eine Basis mit 4 Elementen e_0, e_1, e_2, e_3,

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

so daß

$$e_0 = \mathtt{1}_A \text{ und } e_1^2 = a,\ e_2^2 = b,\ e_1e_2 = -e_2e_1 = e_3.$$

Das Paar von k-Untervektorräumen $A_0 := k\mathtt{1} \oplus ke_3$, $A_1 := ke_1 \oplus ke_2$ definiert auf A eine $\mathbb{Z}/2$-Graduierung.

(d) Sei A eine endlichdimensionale, assoziative k-Algebra. Angenommen es existiert ein invertierbares Element $b \in A^*$, so daß b^2 im Zentrum $Z(A)$ enthalten ist. Dann ist

$$\alpha : A \to A,\ x \mapsto bxb^{-1},$$

ein k-Automorphismus von A der Ordnung 2, und die Eigenräume A_0, A_1 zu 1 bzw. -1 von α definieren eine $\mathbb{Z}/2$-Graduierung von A.

Definition Seien $A = A_0 \oplus A_1$, $B = B_0 \oplus B_1$ $\mathbb{Z}/2$-graduierte k-Algebren. Ein Homomorphismus $f : A \to B$ von k-Algebren heißt *verträglich mit der gegebenen Graduierung* oder *graduierter k-Homomorphismus*, falls $f(A_i) \subset B_i$ für $i = 0, 1$.

Definition Seien $A = A_0 \oplus A_1$, $B = B_0 \oplus B_1$ $\mathbb{Z}/2$-graduierte k-Algebren. Das *graduierte Tensorprodukt* $A\widehat{\otimes}_k B$ ist wie folgt definiert. Es ist

$$A\widehat{\otimes}_k B := A \otimes_k B \quad \text{als } k\text{-Vektorraum}$$

und

$$(A\widehat{\otimes}_k B)_0 := (A_0 \otimes_k B_0) \oplus (A_1 \otimes_k B_1)$$

$$(A\widehat{\otimes}_k B)_1 := (A_0 \otimes_k B_1) \oplus (A_1 \otimes_k B_0),$$

so daß also

$$A\widehat{\otimes}_k B = (A\widehat{\otimes}_k B)_0 \oplus (A\widehat{\otimes}_k B)_1 \quad \text{als } k\text{-Vektorraum}.$$

Die Multiplikation in $A\widehat{\otimes}_k B$ ist wie folgt definiert:

$$(a_i \otimes b_j)(b'_n \otimes b'_l) := (-1)^{jn}(a_i \cdot b'_n) \otimes (b_j \cdot b'_l),$$

wobei $a_i \in A_i$, $b'_n \in A_n$, $b_j \in B_j$, $b'_l \in B_l$.

Das graduierte Tensorprodukt von A und B wird damit zu einer $\mathbb{Z}/2$-graduierten k-Algebra.

Aus der Definition der Multiplikation in $A\widehat{\otimes}_k B$ folgt insbesondere

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

(10.2) $(a_i \otimes 1)(1 \otimes b_j) = (-1)^{ij}(1 \otimes b_j)(a_i \otimes 1)$

für alle $a_i \in A_i$, $b_j \in B_j$.

Ähnlich wie das Tensorprodukt läßt sich auch das graduierte Tensorprodukt durch eine universelle Eigenschaft charakterisieren. Seien dazu $A = A_0 \oplus A_1$ und $B = B_0 \oplus B_1$ $\mathbb{Z}/2$-graduierte k-Algebren und seien

$$\iota_A : A \to A\widehat{\otimes}_k B \ , \quad a \mapsto a \otimes 1$$

$$\iota_B : B \to A\widehat{\otimes}_k B \ , \quad b \mapsto 1 \otimes b$$

die entsprechenden Einbettungen. Ist dann C eine weitere $\mathbb{Z}/2$-graduierte k-Algebra und sind

$$f : A \to C \ , \quad g : B \to C$$

graduierte k-Algebra Homomorphismen, so daß ihre Bilder in C antikommutieren, d.h. es gilt

$$f(a_i)g(b_j) = (-1)^{ij}g(b_j)f(a_i)$$

für alle $a_i \in A_i$, $b_j \in B_j$, dann gibt es genau einen graduierten k-Algebra Homomorphismus

$$h : A\widehat{\otimes}_k B \to C,$$

so daß $f = h \circ \iota_A$ und $g = h \circ \iota_B$. Es gilt

$$h(a\widehat{\otimes}b) = h((a \otimes 1)(1 \otimes b) = h(a \otimes 1)h(1 \otimes b) =$$

$$= h(\iota_A(a))h(\iota_B(b)) = f(a)g(b)$$

für alle $a \in A$, $b \in B$; und

$$f(a_i)g(b_j) = h(a_i \otimes 1)h(1 \otimes b_j) =$$

$$= h((a_i \otimes 1)(1 \otimes b_j)) =$$

$$= h((-1)^{ij}(1 \otimes b_j)(a_i \otimes 1)) =$$

$$= (-1)^{ij}g(b_j)f(a_i)$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

für alle $a_i \in A_i$, $b_j \in B_j$.

Wir wollen nun jedem endlichdimensionalen k-Vektorraum V, der mit einer nichtausgearteten quadratischen Form $q : V \to k$ versehen ist, eine $\mathbb{Z}/2$-graduierte k-Algebra $C(V, q)$, die sogenannte *Cliffordalgebra von* (V, q), zuordnen. Sei dazu

$$T(V) := \oplus_{n\in\mathbb{Z}} V^{\otimes n}$$

die sogenannte *Tensoralgebra von* V; dabei ist $V^{\otimes n} := \{0\}$ für $n < 0$, $V^{\otimes 0} := k$ und $V^{\otimes n}$ das n-fache Tensorprodukt von V über k mit sich selbst; in $T(V)$ gilt

$$(x_1 \otimes ... \otimes x_m)(y_1 \otimes ... \otimes y_n) = x_1 \otimes ... \otimes x_m \otimes y_1 \otimes ... \otimes y_n$$

für alle $x_1, ..., x_m,\ y_1, ..., y_n \in V$. Die Tensoralgebra läßt sich durch eine universelle Eigenschaft charakterisieren. Sei dazu $\iota : V \to T(V)$, $v \mapsto v$, die kanonische Einbettung; manchmal schreiben wir auch $\iota(v) = v$. Sei A eine k-Algebra und sei $f : V \to A$ ein k-Homomorphismus von Vektorräumen. Dann gibt es genau einen Homomorphismus von k-Algebren $g : T(V) \to A$ mit $f = g \circ \iota$. Dabei gilt

$$g(x_1 \otimes ... \otimes x_n) = f(x_1) \cdots f(x_n)$$

für alle $x_1, ..., x_n \in V$. Die Tensoralgebra $T(V)$ wird durch

$$T(V)_0 := \oplus_{n\ gerade} V^{\otimes n},\ \ T(V)_1 := \oplus_{n\ ungerade} V^{\otimes n}$$

zu einer $\mathbb{Z}/2$-graduierten k-Algebra mit $k \subset T(V)_0$.

Definition Sei (V, q) ein nichtausgearteter quadratischer Raum über dem Körper k mit $char(k) \neq 2$. V ist also ein endlichdimensionaler k-Vektorraum mit einer Abbildung $q : V \to k$, so daß

$$q(cv) = c^2 q(v) \quad \text{für alle} \quad c \in k,\ v \in V,$$

und so daß die Abbildung

$$b_q : V \times V \to k,\ b_q(v, w) := \tfrac{1}{2}(q(v + w) - q(v) - q(w)),\ v, w \in V,$$

eine nichtausgeartete symmetrische Bilinearform ist.

Sei $I(q)$ das zweiseitige Ideal in $T(V)$, das erzeugt wird von allen Elementen der Form

$$v \otimes v - q(v),\ v \in V.$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Die Quotientenalgebra

$$C(V, q) := T(V)/I(q)$$

heißt die *Clifford-Algebra von* (V, q).

Die Clifford-Algebra läßt sich durch eine universelle Eigenschaft charakterisieren. Sei dazu $- : T(V) \to C(V, q)$ der entsprechende Restklassenhomomorphismus und sei

$$\kappa : V \xrightarrow{\iota} T(V) \xrightarrow{-} C(V, q)$$

die Zusammensetzung von ι mit $-$. Dann gilt in $C(V, q)$

(10.3) $\quad \kappa(v)^2 = 1 \cdot q(v)$ für alle $v \in V$.

Sei A eine k-Algebra und sei $f : V \to A$ ein k-Homomorphismus von k-Vektorräumen mit der Eigenschaft

$$f(v)^2 = 1 \cdot q(v) \text{ für alle } v \in V.$$

Dann existiert genau ein k-Homomorphismus von k-Algebren

$$g : C(V, q) \to A, \text{ so daß } f = g \circ \kappa.$$

Man erhält g wie folgt. Aus der universellen Eigenschaft der Tensoralgebra folgt zunächst die Existenz eines eindeutigen Homomorphismus von k-Algebren $h : T(V) \to A$ mit der Eigenschaft $h \circ \iota = f$. Für alle $v \in V$ ist

$$h(v \otimes v - 1q(v)) = h(v \otimes v) - 1q(v) = f(v)^2 - 1q(v) = 0.$$

Also ist das Ideal $I(q)$ im Kern von h enthalten, d.h. h faktorisiert über $C(V, q)$. Definiert man daher

$$g : C(V, q) \to A, \; a + I(q) \mapsto h(a),$$

dann gilt $f = h \circ \iota = g \circ \kappa$.

Um die Schreibweise zu vereinfachen, werden Elemente aus V als Elemente aus $T(V)$ und manchmal sogar als Elemente aus $C(V, q)$ aufgefaßt; und die Abbildung $\kappa : V \to C(V, q)$ wird durch die Schreibweise $v \mapsto \overline{v}$ angedeutet.

(10.4) **Bemerkungen** (a) Sei

$$b_q : V \times V \to k, \; b_q(v, w) := \tfrac{1}{2}(q(v + w) - q(v) - q(w)), \; v, w \in V,$$

die zu q gehörige nichtausgeartete symmetrische Bilinearform. Für $v, w \in V$ schreiben wir auch $v \perp w$ für $b_q(v, w) = 0$. Aus $v \perp w$ folgt

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$\overline{vw} = -\overline{wv}$;

denn in $C(V,q)$ gilt $\overline{v}^2 = 1 \cdot q(v)$ und $\overline{w}^2 = 1q(w)$. Wenn also

$0 = b_q(v,w) = \frac{1}{2}(q(v+w) - q(v) - q(w)),$

dann ist

$\overline{v}^2 + \overline{w}^2 = q(v) + q(w) = q(v+w) = (\overline{v} + \overline{w})^2 = \overline{v}^2 + \overline{vw} + \overline{wv} + \overline{w}^2,$

also

$\overline{vw} + \overline{wv} = 0.$

(b) Wenn $v \in V$ bezüglich q anisotrop ist, d.h. wenn $q(v) \neq 0$ ist, und wenn $\overline{v} \in C(V,q)$ invertierbar ist, dann gilt

$\overline{v}^{-1} = \overline{v} \cdot q(v)^{-1};$

denn

$\overline{v}(\overline{v})^{-1} = \overline{vv}q(v)^{-1} = q(v)q(v)^{-1} = 1.$

(c) Ist δ ein k-Automorphismus von (V,q), d.h. ein k-Automorphismus von V mit der Eigenschaft $q \circ \delta = q$, dann gilt $I(q \circ \delta) = I(q)$, und δ induziert aufgrund der universellen Eigenschaft der Clifford-Algebra einen Automorphismus von k-Algebren

$\overline{\delta} : C(V,q) \to C(V,q),$

so daß $\overline{\delta} \circ - = f$, wobei

$f : V \xrightarrow{\delta} V \xrightarrow{-} C(V,q)$

die Zusammensetzung von δ mit dem k-Vektorraumhomomorphismus

$V \xrightarrow{-} C(V,q),\ v \mapsto \overline{v},$

ist.

Wir wollen nun auf der Clifford-Algebra eine $\mathbb{Z}/2-$Graduierung definieren. Dazu bemerken wir zunächst, daß das zweiseitige Ideal $I(q)$ aus $T(V)$ durch Elemente aus $T(V)_0$ erzeugt wird; denn es gilt

$(v \otimes v - q(v)) \in k \oplus V^{\otimes 2} \subset T(V)_0.$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Mit

$I(q)_0 := T(V)_0 \cap I(q)$, $I(q)_1 := T(V)_1 \cap I(q)$

gilt

$I(q) = I(q)_0 \oplus I(q)_1$

und

$C(V,q) = T(V)_0/I(q)_0 \oplus T(V)_1/I(q)_1,$

jeweils als k-Vektorräume. Wir setzen

$C(V,q)_0 := T(V)_0/I(q)_0, \;\; C(V,q)_1 := T(V)_1/I(q)_1,$

und erhalten damit eine $\mathbb{Z}/2$-Graduierung von $C(V,q)$. Man nennt $C(V,q)_0$ die *gerade Clifford Algebra* und, obwohl es sich dabei i.a. nicht um eine Algebra handelt, $C(V,q)_1$ die *ungerade Clifford Algebra* oder *den ungeraden Anteil der Clifford Algebra.*

Die folgende Abbildung ist ein Isomorphismus von k-Algebren

(10.5) $\quad C(V,q)_0 \oplus C(V,q)_1 \stackrel{\cong}{\to} C(V,q)$

$$(t_0 + I(q)_0, t_1 + I(q)_1) \mapsto (t_0 + t_1 + I(q)_o + I(q)_1)$$

Außerdem beweist man unter Benutzung der universellen Eigenschaft der Clifford-Algebra, daß für nichtausgeartete quadratische Räume $(V_1,q_1);(V_2,q_2)$ die Abbildung

$V_1 \oplus V_2 \to C(V_1,q_1)\widehat{\otimes}_k C(V_2,q_2)$

$v_1 \oplus v_2 \mapsto \overline{v}_1 \otimes 1 + 1 \otimes \overline{v}_2$

einen Isomorphismus von k-Algebren induziert:

(10.6) $\;C((V_1,q_1) \perp (V_2,q_2)) \stackrel{\cong}{\to} C(V_1,q_1)\widehat{\otimes}_k C(V_2,q_2);$

dabei bezeichnet $(V_1,q_1) \perp (V_2,q_2)$ die orthogonale Summe von (V_1,q_1) und (V_2,q_2).

(10.7) **Beispiel** Sei $V = kx$ ein 1-dimensionaler k-Vektorraum mit der quadratischen Form $q : V \to k$, so daß $q(x) = \alpha \in k^*$. Dann existiert ein Isomorphismus von k-Algebren

$C(V,q) \cong k\,[t]\,/(t^2 - \alpha) \cong k \oplus kx$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

wie man folgendermaßen erkennt: Die Abbildungen

$\Phi_n : k \otimes ... \otimes k \to k,\ x_1 \otimes ... \otimes x_n \mapsto x_1 x_2 ... x_n$

$\Psi_m : k \oplus ... \oplus k \to k\,[t]\,, (x_1, ..., x_m) \mapsto x_1 + x_2 t + ... + x_m t^{m-1}$

induzieren einen Isomorphismus von k-Algebren

$$\begin{aligned} T(V) = \oplus_{n \geq 0} V^{\otimes n} &= k \oplus k \oplus (k \otimes k) \oplus (k \otimes k \otimes k) \oplus ... \\ &\cong k \oplus k \oplus k \oplus k \oplus ... \\ &\cong k\,[t] \end{aligned}$$

Wegen $q(x) = \alpha$ ist $I(q) = \langle x \otimes x - q(x) : x \in V \rangle = (t^2 - \alpha)$, d.h. $I(q)$ ist das von dem Polynom $t^2 - \alpha$ erzeugte Hauptideal in $k\,[t]\,.$

(10.8) **Satz** *Sei (V, q) ein n-dimensionaler quadratischer Raum über k mit der Orthogonalbasis $e_1, ..., e_n$. Dann gilt*

(a) $\dim_k C(V, q) = 2^n$

(b) *Die Produkte der Form*

$\overline{e}_1^{\epsilon_1} \cdots \overline{e}_n^{\epsilon_n}$ *mit* $\epsilon_i \in \{0, 1\}$

bilden eine Vektorraumbasis von $C(V, q)$

(c) *Der Vektorraumhomomorphismus*

$V \to C(V, q),\ v \mapsto \overline{v},$

ist injektiv.

Beweis: Zu (a): Für $n = 1$ folgt aus Beispiel (10.7):

$\dim_k(C(V, q)) = \dim_k(k \oplus kx) = 2.$

Bezeichnet (V_i, q_i) den 1-dimensionalen quadratischen Raum mit der Basis e_i, dann folgt aus (10.6):

$V(V, q) \cong C(V_1.q_1) \widehat{\otimes}_k ... \widehat{\otimes}_k C(V_n, q_n).$

Daraus ergibt sich Behauptung (a).

Zu (b): Die Basiselemente $e_1, ..., e_n \in V$ erzeugen $T(V)$ als k-Algebra, und deren Bilder $\overline{e}_1, ..., \overline{e}_n$ in $C(V, q)$ erzeugen daher $C(V, q)$ als k-Algebra. Alle Produkte der $\overline{e}_i$ sind von der Form $\overline{y} = \overline{y}_1 ... \overline{y}_m$ mit $y_i \in \{e_1, ..., e_n\}$. Wegen der Orthogonalität der Basisvektoren folgt nach Bemerkung (10.4), Teil (a), daß

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$\overline{e}_i\overline{e}_j = -\overline{e}_j\overline{e}_i$ für alle $i, j \in \{1, ..., n\}$.

Außerdem gilt

$\overline{e}_i^2 = q(e_i)$ für alle $i \in \{1, ..., n\}$.

Es folgt

$\overline{y} = \gamma\overline{e}_1^{\epsilon_1} \cdots \overline{e}_n^{\epsilon_n}$ mit $\gamma \in k^*$ und $\epsilon_i \in \{0, 1\}$.

Auf diese Weise ergeben sich 2^n linear unabhängige erzeugende Elemente. Wegen $\dim_k(C(V, q)) = 2^n$ folgt die Behauptung.

Zu (c): Schreibt man $v \in V$ in der Form $v = a_1e_1 + ... + a_ne_n$ und ist $\overline{v} = a_1\overline{e}_1 + ... + a_n\overline{e}_n = \overline{0}$ in $C(V, q)$, dann folgt aus der linearen Unabhängigkeit der $\overline{e}_i$ in $C(V, q)$, daß alle $a_i = 0$ und damit $v = 0$ ist.

Damit ist der Beweis von (10.8) beendet.

(10.9) **Bemerkung** Mit den Bezeichnungen von (10.8) bilden die Elemente der Form

$\overline{e}_1^{\epsilon_1} \cdots \overline{e}_n^{\epsilon_n}$ mit $\epsilon_i \in \{0, 1\}$ und $\sum_{i=1}^{n} \epsilon_i \equiv 0 \bmod 2$

eine k-Vektorraumbasis von $C(V, q)_0$. Es folgt, daß das Zentrum von $C(V, q)_0$ isomorph zu k ist.

Zur Clifford-Algebra $C = C(V, q)$ bilden wir die entgegengesetzte Algebra C^{op}, d.h. es ist $C^{op} = C$ als k-Vektorraum, und für $x, y \in C$ ist xy in C^{op} gleich yx in C. Für Elemente $v_1, ..., v_n \in V$ sei

$I(\overline{v}_1 \cdots \overline{v}_n) := \overline{v}_n \cdots \overline{v}_1$.

Dadurch wird ein Vektorraumisomorphismus $I : C \to C^{op}$ mit den folgenden Eigenschaften definiert:

$I^2 = id$, $I(xy) = I(y)I(x)$ für alle $x, y \in C$

I heißt der *kanonische Antiautomorphismus von C*. Für $e \in V$ sei

$H_e := \{v \in V : b_q(v, e) = 0\}$;

H_e ist ein Untervektorrraum von V, die sogenannte *zum Vektor e senkrechte Hyperebene*. Es gilt

$V = ke \perp H_e$.

Die k-lineare Abbildung

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$s_e : V \to V$ mit $s_e(e) = -e$ und $s_e(h) = h$ für alle $h \in H$

ist eine Isometrie von q, d.h. es gilt $q \circ s_e = q$, mit der Eigenschaft $s_e^2 = id$; s_e heißt die *Spiegelung auf V an der zum Vektor e senkrechten Hyperebene H_e*. Bezüglich einer geeigneten Basis von V ist die Matrix von s_e gegeben durch

$$\begin{pmatrix} 1 & & & & & & \\ & \cdot & & & & & \\ & & \cdot & & & & \\ & & & \cdot & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & -1 \end{pmatrix}.$$

Die Determinante von s_e ist also gleich -1. Wir teilen nun ein für die Theorie der quadratischen Formen wichtiges Resultat über die Erzeugbarkeit der orthogonalen Gruppe

$$O(q) := O(V, q) := \{\delta \in Aut_k(V) : q \circ \delta = q\}$$

und der speziellen orthogonalen Gruppe

$$SO(q) := \{\delta \in O(q) : \det(\delta) = 1\}$$

durch Spiegelungen ohne Beweis mit, vgl. z. B. [CH].

(10.10) **Satz** (Cartan, Dieudonné, Witt) (a) *Jedes Element aus $SO(q)$ ist Produkt einer geraden Anzahl von Spiegelungen.*

(b) *Ist $n = \dim V$, dann ist jedes Element aus $O(q)$ Produkt von höchstens n Spiegelungen.*

Wir benötigen eine Beschreibung von Spiegelungen innerhalb der Clifford-Algebra. Sei dazu s_e die Spiegelung auf V an der zu $e \in V$ senkrechten Hyperebene H_e und sei

$$\overline{s}_e : C \to C$$

der durch s_e induzierte Automorphismus der Clifford-Algebra $C = C(V, q)$. Dann gilt

(10.11) $\overline{s}_e(x) = -\overline{e}x\overline{e}^{-1}$ für alle $x \in C$.

Denn für alle $\alpha \in k$ gilt $\overline{s}_e(\alpha\overline{e}) = -\alpha\overline{e} = -\overline{e}\alpha\overline{e}\overline{e}^{-1}$, und für $v \in H_e$ gilt nach Bemerkung (10.4), Teil (a): $\overline{ve} = -\overline{ev}$, also $-\overline{eve}^{-1} = \overline{v} = \overline{s}_e(\overline{v})$.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Definition Die sogenannte *gerade Clifford-Gruppe zu* (V, q) ist definiert durch

$$\Gamma_0 := \Gamma_0(q) := \{s \in C_0^* : s\overline{V}s^{-1} = \overline{V}\};$$

dabei bezeichnet $\overline{V}$ das Bild von V in $C = C(V, q)$.

Die Abbildung

$$\alpha : \Gamma_0 \to Aut_k(V),\ s \mapsto \alpha_s,$$

wobei der k-Automorphismus $\alpha_s : V \to V$ durch die entsprechende Abbildung

$$\overline{V} \to \overline{V},\ \overline{v} \mapsto s\overline{v}s^{-1},$$

definiert ist, ist ein Gruppenhomomorphismus. Es folgt: $\alpha_s \in O(q)$; denn $q(\alpha_s(v)) = (\overline{\alpha_s(v)})^2 = s\overline{v}^2 s^{-1} = sq(v)s^{-1} = q(v)$ für alle $v \in V$. Somit erhalten wir einen Gruppenhomomorphismus

$$(10.12) \quad \alpha : \Gamma_0 \to O(q),\ s \mapsto \alpha_s.$$

(10.13) **Bemerkungen** (a) Für eine gerade Anzahl von Elementen $v_1, ..., v_{2q} \in V$ ist $s := \overline{v}_1 \cdots \overline{v}_{2q} \in C_0$ und $\alpha_s = \alpha_{\overline{v}_1} \cdots \alpha_{\overline{v}_{2q}}$ Produkt einer geraden Anzahl von Spiegelungen. Also ist $\alpha_s \in SO(q)$.

(b) Für $\delta \in O(q)$ sei $\overline{\delta} \in Aut_k(C(V, q))$ der durch δ induzierte Automorphismus der Clifford Algebra. Man erhält einen Gruppenhomomorphismus

$$\overline{\alpha} : \Gamma_0 \xrightarrow{\alpha} O(q) \xrightarrow{-} \{\alpha \in Aut_k(C) : \alpha_{|V} \in Aut_k(V)\}$$

mit

$$\overline{\alpha}(s) = \overline{\alpha}_s \quad \text{für alle} \quad s \in \Gamma_0.$$

Über den Homomorphismus α aus (10.12) gilt der folgende Satz, vgl. $[CH]$.

(10.14) **Satz** *Das Bild von α ist $SO(q)$, und der Kern von α ist k^*.*

Aus der vorangehenden Bemerkung (10.13), Teil (a), ergibt sich, daß das Bild von α in $SO(q)$ enthalten ist. Umgekehrt: Jedes Element aus $SO(q)$ ist Produkt einer geraden Anzahl von Spiegelungen, also nach (10.11) Konjugation mit einem Element aus C_0^* und damit insbesondere im Bild von α enthalten. Der Kern von α besteht aus allen $s \in \Gamma_0$, so daß $s\overline{v}s^{-1} = \overline{v}$ für alle $v \in V$. Daraus folgt, daß s im Zentrum von C_o, also in k, enthalten ist.

Definition Die *Spinornorm* ist die Abbildung

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$SN : SO(q) \to k^*/k^{*2},\ t \mapsto I(p)p \cdot k^{*2},$

wobei $t = s_{v_1} \cdots s_{v_{2q}}$ Produkt einer geraden Anzahl von Spiegelungen zu $v_1, ..., v_{2q} \in V$ und $p := \overline{v}_1 \cdots \overline{v}_{2q}$ das entsprechende Element in $C = C(V, q)$ ist, also

$$I(p)p = \overline{v}_{2q} \cdots \overline{v}_1 \overline{v}_1 \cdots \overline{v}_{2q} = q(v_1) \cdots q(v_{2q}) \in k^*.$$

(p ist bis auf ein Element aus $Kern(\alpha) = k^*$ durch t eindeutig bestimmt.)

Der Kern $Kern(SN)$ der Spinornorm besteht aus allen $t \in SO(q)$, die sich in der Form

$$t = s_{v_1} \cdots s_{v_{2q}} \quad \text{mit } v_1, ..., v_{2q} \in V \quad \text{und} \quad q(v_1) \cdots q(v_{2q}) \in k^{*2}$$

darstellen lassen.

Definition Die *Spingruppe von* (V, q) ist

$$Spin(V, q) := Spin(q) := \{p \in \Gamma_0 : I(p)p = 1\}.$$

Somit induziert der Gruppenhomomorphismus $\alpha : \Gamma_0 \to SO(q)$ einen Gruppenhomomorphismus

$$\alpha_{|Spin} : Spin(V, q) \to Kern(SN)$$

mit dem Kern $\{\pm 1\} =: \mu_2 \leq k^*$; es besteht also die exakte Sequenz

$$1 \to \mu_2 \to Spin(V, q) \stackrel{\alpha_{|Spin}}{\to} Kern(SN).$$

Wenn $k^* = k^{*2}$ gilt, dann ist $Kern(SN) = SO(V, q)$ und $\alpha_{|Spin}$ ist surjektiv; vgl. (10.14). Zusammenfassend läßt sich also feststellen

(10.15) **Bemerkung** Ist der Körper k quadratisch abgeschlossen, d.h. gilt $k^* = k^{*2}$, dann besteht die folgende exakte Sequenz

$$1 \to \mu_2 \to Spin(V, q) \stackrel{\alpha_{|Spin}}{\to} SO(V, q) \to 1;$$

$Spin(V, q)$ ist also eine zentrale Erweiterung von $SO(V, q)$ mit dem Kern μ_2

Nachfolgend wird beschrieben, wie sich diese Überlegungen bei der Klassifikation quadratischer Formen einsetzen lassen, vgl. [SR] sowie [$SE2$], Chapter III, §3, (3.2), Example b. Sei also nach wie vor k ein Körper mit $char(k) \neq 2$ und sei (V, q) ein nichtausgearteter quadratischer Raum der Dimension n. Sei K/k eine Galoiserweiterung mit der Galoisgruppe G, so daß $K^* = K^{*2}$,d.h.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

K ist quadratisch abgeschlossen. Die Automorphismengruppe $Aut((V_K, q_K))$ ist die orthogonale Gruppe $O((V_K, q_K)) = O(q_K)$, und wir haben die in (8.9) erklärte Bijektion

$$\theta : E_{(V,q)}(K/k) \rightarrow H^1(G, O(q_K)).$$

Weil K quadratisch abgeschlossen ist, ist q_K isomorph zur Einheitsform

$$q_e : X_1^2 + ... + X_n^2.$$

Ist T eine auf Einheitsform transformierende Matrix, dann ist die Abbildung

$$O(q_K) \rightarrow O(q_{e,K}),\ S \mapsto TST^t$$

ein Isomorpphismus von G-Gruppen und daher die dadurch induzierte Abbildung von Kohomologiemengen

$$H^1(G, O(q_K)) \rightarrow H^1(G, O(q_{e,K}))$$

eine Bijektion. Deshalb sei im Folgenden $q = q_e$ die Einheitsform der Dimension n. Die exakte Sequenz

$$1 \rightarrow SO(q_K) \rightarrow O(q_K) \stackrel{\det}{\rightarrow} \mu_2 \rightarrow 1$$

ist eine exakte Sequenz von G-Gruppen und induziert daher die folgende exakte Sequenz von punktierten Kohomologiemengen

$$H^0(G, \mu_2) \stackrel{\delta}{\rightarrow} H^1(G, SO(q_K)) \rightarrow H^1(G, O(q_K)) \stackrel{\det}{\rightarrow} H^1(G, \mu_2).$$

Weil G auf μ_2 trivial operiert, ist $H^0(G, \mu_2) = \mu_2$. Außerdem ist

$$H^1(G, \mu_2) \cong k^*/k^{*2}.$$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Also haben wir die exakte Sequenz von Kohomologiemengen

(10.16) $\mu_2 \xrightarrow{\delta} H^1(G, SO(q_K)) \to H^1(G, O(q_K)) \xrightarrow{\det} k^*/k^{*2}$

Sie eröffnet die Möglichkeit, $H^1(G, O)(q_K))$ und damit $E_{(V,q_e)}(K/k)$ mit Hilfe von $H^1(G, SO(q_K))$ zu bestimmen. Um $H^1(G, SO(q_K))$ zu beschreiben, stellt man zunächst fest, daß die exakte Sequenz aus (10.15) über K, also

$1 \to \mu_2 \to Spin(q_K) \to SO(q_K) \to 1,$

eine exakte Sequenz von G-Gruppen ist. Somit erhält man aufgrund von (4.6) die exakte Sequenz von punktierten Kohomologiemengen

$H^0(G, Spin(q_K)) \to H^0(G, SO(q_K)) \xrightarrow{\delta} H^1(G, \mu_2) \to H^1(G, Spin(q_K)) \to$

$\to H^1(G, SO(q_K)) \xrightarrow{\Delta} H^2(G, \mu_2),$

also wegen

$H^1(G, \mu_2) \cong k^*/k^{*2}$ und $H^2(G, \mu_2) \cong Br_2(k)$

die exakte Sequenz von punktierten Kohomologiemengen

$Spin(q) \to SO(q) \to k^*/k^{*2} \to H^1(G, Spin(q_K)) \to H^1(G, SO(q_K)) \to$

$\to Br_2(k)$

Unter der Voraussetzung

(10.17) $H^1(G, Spin(q_K)) = 1,$

die für Körper k, deren kohomologische 2-Dimension nicht größer als 2 ist, erfüllt ist, vgl. dazu $[SE2]$, Chapter III, 3.2, (b), p. 141, in Verbindung mit $[MK2]$, $[BP]$, hat also die Abbildung

$H^1(G, SO(q_K)) \to Br_2(k)$

trivialen Kern. Zusammen mit der obigen exakten Sequenz

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$$\mu_2 \to H^1(G, SO(q_K)) \to H^1(G, O(q_K)) \stackrel{\det}{\to} k^*/k^{*2}$$

erhält man damit eine Möglichkeit, für Körper k, die die Voraussetzung (10.17) erfüllen, $H^1(G, O(q_K))$ und damit die Menge $E_{(V,q)}(K/k)$ zu bestimmen.

Das durch die obige Korandabbildung Δ für jedes Element aus $H^1(G, SO(q_K))$ definierte Element in der Brauergruppe $Br(k)_2$ ist Beispiel einer kohomologischen Invariante, die mit der sogenannten Hasse-Witt Invariante zusammenhängt; vgl. dazu auch [SR], 4.7, p. 251, sowie [$SE2$], Appendix 2, §2. Kohomologischen Invarianten quadratischer Formen werden in [AN], [DZ] , [SR] , [$SC1$] eingeführt und untersucht. Die einflußreiche Arbeit [$MN2$] stellt Zusammenhänge zwischen quadratischen Formen, der Brauergruppe und der algebraischen K-Theorie her; vgl. dazu auch den Übersichtsartikel [PF] und die grundlegenden Resultate von V. Voevodsky, vgl. z.B. [$V1$], [$V2$]. Die Resultate in [$MK1$] und [$MK2$] sind von grundlegender Bedeutung für den Zusammenhang zwischen quadratischen Formen und der Brauergruppe. In dem Übersichtsartikel [BF] findet man weitere Resultate über kohomologische Invarianten, die mit quadratischen Formen zusammenhängen. Für Zusammenhänge zwischen Hasse-Witt Invarianten von Spurformen und Einbettungsproblemen vgl. [$SE4$], §3, sowie [$SE3$], 9. Für eine allgemeine Theorie von kohomologischen Invarianten vgl. [GMS], "Chomological invariants, Witt invariants and trace forms", und die dort genannte Literatur.

Aufgaben und Beispiele

(1) Sei q_e die n-dimensionale quadratische Einheitsform über einem Körper k. Zeigen Sie, daß zu jedem $(\alpha) \in H^1(G(\overline{\mathbb{Q}}/\mathbb{Q}), SO(q_e))$ ein $m \in \mathbb{N}$ existiert, so daß $\mathbb{Q}(\mu_m)$ ein Zerfällungskörper für (α) ist. (Wohlbekannt; quadratische Gaußsche Summen anwenden)

(2) Zeigen Sie: Ist q eine nichtausgeartete quadratische Form auf einem $\mathbb{Q}$-Vektorraum V der Dimension ≥ 3, dann existieren ein $t \in \mathbb{N}$ und ein $v \in V \otimes \mathbb{Q}(e^{2\pi i/2^t})$, $v \neq o$, so daß $q_{\mathbb{Q}(e^{2\pi i/2^t})}(v) = 0$. (Vgl. [$ST$])

§ 11. Twistungen von Körpern

In diesem Abschnitt folgen wir weitgehend entsprechenden Ausführungen in [$H1$], 4.4; [RQ]; [$SE1$], Chapter X, §6; diese Ausführungen basieren ihrerseits in Teilen auf den grundlegenden Arbeiten [$WT3$]; [$C1$],[$C2$]; [AMT].

Sei k ein Körper und sei $\overline{k}$ ein separabler algebraischer Abschluß von k. Sei $\mathfrak{G}(k)$ eine Kategorie von Körpererweiterungen K/k in $\overline{k}$. Für $K \in Ob(\mathfrak{G}(k))$ heißt eine Körpererweiterung E von k linear disjunkt zu K über k, falls jede endliche Teilmenge aus K, die über k linear unabhängig ist, auch über E linear unabhängig ist, so daß also die k-Algebra $E_K := E \otimes_k K$ ein Körper ist, der in einem gemeinsamen Oberkörper von E und K isomorph zum Kompositum von E mit K ist, vgl. z.B. [BK]. Zum Beispiel ist der Körper der rationalen Funktionen $E = k(t)$ in einer Unbestimmten t über k linear disjunkt zu jedem

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$K \in Ob(\mathfrak{G}(k))$, und es gilt $k(t) \otimes_k K = K(t)$. Sei $\mathfrak{F}_k$ die Kategorie, deren Objekte die Körpererweiterungen von k sind, die zu allen $K \in Ob(\mathfrak{G}(k))$ linear disjunkt sind, und deren Morphismen die k-Homomorphismen sind. Für jedes $M \in Ob(\mathfrak{G}(k))$ sei $\mathfrak{F}_M$ die entsprechend gebildete Kategorie zu M. Für je zwei Objekte $K, L \in Ob(\mathfrak{G}(k))$, so daß L/K eine Körpererweiterung ist, sei $r_{L/K} : \mathfrak{F}_K \to \mathfrak{F}_L$ der Funktor, der jedem $E \in Ob(\mathfrak{F}_K)$ das Objekt $E_L := E \otimes_K L \in Ob(\mathfrak{F}_L)$ und jedem Morphismus $f \in Mor(E, F)$ aus $\mathfrak{F}_K$ den Morphismus $f_L \in Mor(E_L, F_L)$,

$$f_L := f \otimes id_L : E_L \to F_L, \ \ e \otimes \lambda \mapsto f(e) \otimes \lambda,$$

aus $\mathfrak{F}_L$ zuordnet. Somit erhalten wir eine durch $\mathfrak{G}(k)$ indizierte Kategorie $\mathfrak{F}$, deren Objekte die Kategorien $\mathfrak{F}_K$ für $K \in Ob(\mathfrak{G}(k))$ und deren Morphismen die Funktoren $r_{L/K} : \mathfrak{F}_K \to \mathfrak{F}_L$ sind; vgl. dazu §1.

Seien $K, L \in Ob(\mathfrak{G}(k))$ so, daß L/K eine endliche Galoiserweiterung ist. Sei $E \in Ob(\mathfrak{F}_K)$. Dann induziert jedes $s \in G(L/K)$ den K-Automorphismus

$$id_E \otimes s : E_L \to E_L, \ \ e \otimes \lambda \mapsto e \otimes s(\lambda).$$

Für $f \in Isom(E_L, F_L)$ und $s \in G(L/K)$ ist dann auch $s \circ f \circ s^{-1} \in Isom(E_L, F_L)$. Wir wollen zeigen, daß $\mathfrak{F}$ fortsetzend ist, d.h. für je zwei Objekte $E, F \in Ob(\mathfrak{F}_K)$ ist $f \in r_{L/K}(Isom(E, F))$ genau dann, wenn $f \in Isom(E_L, F_L)^{G(L/K)}$. Sei also $g \in Isom(E, F)$ mit $f := r_{L/K}(g) = g_L$. Dann ist für alle $s \in G(L/K)$

$$s(g_L) = s \circ g_L \circ s^{-1} = s \circ g \otimes id_L \circ s^{-1} = g \otimes s \circ id_L \circ s^{-1} = g \otimes id_L = g_L,$$

d.h. $f = g_L \in Isom(E_L, F_L)^{G(L/K)}$. Sei umgekehrt $f \in Isom(E_L, F_L)^{G(L/K)}$. Sei (e_i) eine K-Basis von E. Dann ist (e_i) eine L-Basis von E_L. Schreibe $f(e_i) = \Sigma_j a_{ij} e_j$ mit $a_{ij} \in L$. Dann ist $s(f)(e_i) = s(f(s^{-1}(e_i)) = s(f(e_i)) = \Sigma_j s(a_{ij}) e_j = f(e_i) = \Sigma_j a_{ij} e_j$ für alle $s \in G(L/K)$, also alle $a_{ij} \in K$. Setzt man daher $g(e_i) := \Sigma_j a_{ij} e_i$, so ist $f = g_L$.

Damit ist gezeigt

(11.1) **Satz** *Die durch $\mathfrak{G}(k)$ indizierte Kategorie $\mathfrak{F}$ ist eine Galoiskategorie über $\mathfrak{G}(k)$.*

Sei E ein festgewähltes K-Objekt von $\mathfrak{F}$ und sei $L \in Ob(\mathfrak{G}(k))$ eine Körpererweiterung von K. Dann ist in der Bezeichnungsweise von §1 $E_{\mathfrak{F}}(L/K, E)$ die Menge aller K-Isomorphieklasen (F) von K-Objekten F von $\mathfrak{F}$ mit $F_L \cong E_L$. Ist L/K eine endliche Galoiserweiterung, dann ist die Abbildung

(11.2) $\quad \theta : E_{\mathfrak{F}}(L/K, E) \to H^1(G(L/K), Aut(E_L))$

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

gemäß §1 wie folgt definiert: Ist F eine L/K-Twistung von E und ist $f \in Isom(E_L, F_L)$ ein Isomorphismus, dann wird (F) auf die Klasse des 1-Kozykels $p : G(L/K) \to Aut(E_L)$, $s \mapsto p_s := f^1 \circ s(f) = f^{-1} \circ s \circ f \circ s^{-1}$, abgebildet. Es gilt

(11.3) **Satz** *Die Abbildung θ aus (12.2) ist bijektiv.*

Beweis: θ ist nach (1.7) injektiv. Um die Surjektivität von θ zu beweisen, sei $p : G(L/K) \to Aut(E_L), s \mapsto p_s$, ein 1-Kozykel. Sei

$$_pG(L/K) = \{p_s \circ s : \ s \in G(L/K)\} \leq Aut(E_L)$$

die mit p getwistete Galoisgruppe und sei $F \subset E_L$ der Fixkörper unter $_pG(L/K)$. Aus der Galoistheorie folgt, daß E_L/F eine Galoiserweiterung mit der Galoisgruppe $_pG(L/K)$ ist. Der Körper F ist linear disjunkt zu L über K. Um das einzusehen sei $M := \{d_j : 1 \leq j \leq m\}$ ein über K linear unabhängiges System von Elementen aus F. Angenommen M ist über L linear abhängig. Dann gibt es in M ein Element d, so daß $d = \Sigma_{j\in J}\alpha_j d_j$ für eine nichtleere Indexmenge $J \subset \{1, ..., m\}$ und $\alpha_j \in L$ für alle $j \in J$. Für alle Elemente d aus F gilt $(p_s \circ s)(d) = d$ für alle $s \in G(L/K)$, also auch $p_{s^{-1}} \circ s^{-1}(d) = d$ für alle $s \in G(L/K)$. Damit folgt

$$d = \Sigma_{j\in J}\alpha_j d_j = \Sigma_{j\in J}\alpha_j p_{s^{-1}} \circ s^{-1}(d_j) = p_{s^{-1}} \circ s^{-1}(\Sigma_{j\in J} s(\alpha_j) d_j) =$$

$$= \Sigma_{j\in J} s(\alpha_j) d_j,$$

also, da die d_j linear unabhängig über L sind, $\alpha_j = s(\alpha_j)$ für alle $j \in J$ und alle $s \in G(L/K)$. Also liegen alle α_j in K; im Widerspruch zur linearen Unabhängigkeit der d_j über K. F ist also linear disjunkt zu L über K, und somit ist $F \in Ob(\mathfrak{F}_L)$. Um zu erkennen, daß $(F) \in E_{\mathfrak{F}}(L/K, E)$ und daß (F) unter θ auf $(p) \in H^1(G(L/K), Aut(E_L))$ abgebildet wird, schließen wir folgendermaßen. Sei $u_1, ..., u_n$ eine K-Basis von L/K. Dann ist $F_L = F(u_1, ..., u_n)$ in E_L enthalten, und E_L/F und F_L/F sind Erweiterungen vom Grad n. Also sind E_L und F_L als Mengen gleich. Ist $x = \Sigma_i d_i u_i \in F_L$, dann ist

$$s(x) = \Sigma_i d_i s(u_i) = \Sigma_i (p_s \circ s)(d_i) s(u_i) = \Sigma_i (p_s \circ s)(\Sigma_j e_{ij} u_j) s(u_i) =$$

$$= \Sigma_{i,j} p_s(e_{ij}) s(u_j u_i) = (p_s \circ s)(\Sigma_i (\Sigma_j e_{ij} u_j) u_i) = p_s \circ s(x),$$

d.h. F_L ist die Twistung von E_L mit p. Die Behauptung folgt.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Sei $K(\underline{x}) = K(x_1, ..., x_m)$ der Körper der rationalen Funktionen in m Unbestimmten $x_1, ..., x_m$ über K; $K(x_1, ..., x_m)$ ist ein K-Objekt von $\mathfrak{F}$. Sei L/K eine endliche Galoiserweiterung mit Galoisgruppe G und sei $L(\underline{x}) = L(x_1, ..., x_m)$ der Körper der rationalen Funktionen in m Unbestimmten über L. Dann ist, mit obigen Bezeichnungen, $L(\underline{x})$ die Skalarerweiterung von $K(\underline{x})$ mit L. Die allgemeine lineare Gruppe $GL(m, L)$ operiert auf $L(\underline{x})$ durch Variablentransformation:

$$t_a : x_i \mapsto \Sigma_{j=1}^m x_j a_{ij}, \;\; i = 1, ..., m, \;\; a = (a_{ij}) \in GL(m, L).$$

Dadurch wird ein Homomorphismus

$$t : GL(m, L) \to Aut(L(\underline{x})), \; a = (a_{ij}) \mapsto t_a,$$

induziert. Sei $L(\underline{y}) = L(y_1, ..., y_{m-1})$ der Körper der rationalen Funktionen in $m-1$ Veränderlichen über L. $L(\underline{y})$ ist Skalarerweiterung von $K(\underline{y}) = K(y_1, ..., y_{m-1})$ mit L. Die Zuordnung $y_i \mapsto \frac{x_i}{x_{m-1}}; i = 1, ..., m-1$, induziert eine Einbettung von $L(\underline{y})$ in $L(\underline{x})$. Aus der Definition von t ergibt sich, daß der Teilkörper $L(\underline{y})$ von $L(\underline{x})$ unter der Operation von $GL(m, L)$ in sich überführt wird, und die Einschränkung des L-Automorphismus $t_a \in Aut_L(L(\underline{x})), a \in GL(m, L)$, von $L(\underline{x})$ auf $L(\underline{y})$ ist ein L-Automorphismus von $L(\underline{y})$. L^* wird durch $c \mapsto c \cdot Id_m$, $Id_m =$ Einheitsmatrix vom Grad m, zu einer Untergruppe von $GL(m, L)$. Es ist offentsichtlich, daß L^* trivial auf $L(\underline{y})$ operiert. Somit erweist sich $GL(m, L)/L^* = PGL(m, L^*)$ als Gruppe von L-Automorphismen von $L(\underline{y})$. Die Operation von $G(L/K)$ auf L induziert eine Operation von $G(L/K)$ auf $L(\underline{y})$, wobei für alle $s \in G(L/K)$ und alle $i \in \{1, ..., m-1\}$ gilt: $s(y_i) := y_i$. Außerdem wird $PGL(m, L)$ durch die Operation von $G(L/K)$ auf L zu einer $G(L/K)$-Gruppe, und als solche eine Untergruppe der $G(L/K)$-Gruppe aller L-Automorphismen von $L(\underline{y})$.

Definition (vgl. [*RQ*], §5) Ein *Brauerkörper* F der Dimension $m-1$ über K ist eine L/K-Twistung F des rationalen Funktionenkörpes in $m-1$ Unbestimmten $K(\underline{y}) = K(y_1, ..., y_{m-1})$ mit einem 1-Kozykel $p : G(L/K) \to PGL(m, L)$.

Aufgrund von (12.3) ist F der Fixkörper von $L(\underline{y})$ unter der Gruppe ${}_pG(L/K)$, vgl. § 3.

Die in §4 unter Aufgaben und Beispiele, (10), erläuterte Charakterisierung der Elemente der Kohomologiemenge $H^1(G(L/K), PGL(m, L))$ durch $GL(m, L)$-Konjugationsklassen von Untergruppen U des semidirekten Produktes

$$\overline{GL(m, L)} = GL(m, L) \times_s G(L/K),$$

für die gilt

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

$U \cap GL(m,L) = L^*$, $GL(m,L) \cdot U = \overline{GL(m,L)}$,

erlaubt eine weitere Charakterisierung von Brauerkörpern, vgl. dazu $[RQ]$, §4, §5. Für grundlegende und weitergehende Resultate über Brauerkörper vgl. $[AMT]$, II, §9-§12, und $[RQ]$, §5-§9.

Der Klasse eines Brauerkörpers entspricht die Isomorphieklasse einer projektiven Varietät, einer sogenannten *Brauer-Severi Varietät.* Solche Varietäten wurden von F. Chatelet unter dem Namen *Brauer-Varietät* eingeführt und untersucht; vgl. $[C1]$, $[C2]$.

Definition (Vgl. $[C1]$;$[C2]$; $[AMT]$, II, 12; $[SE1]$, Chapter X, § 10) Sei k ein Körper. Eine *Brauer-Severi Varietät über* k ist eine über k definierte projektive Varietät, die über einer endlichen separablen Erweiterung des Grundkörpers isomorph zu einem projektiven Raum ist.

Dieser Zusammenhang zwischen den Elementen von $H^1(G(L/K), PGL(m,L))$ und Brauer-Severi Varietäten ist eine unmittelbare Folgerung aus der Deutung der projektiven linearen Gruppe $PGL(m,L)$ als Automorphismengruppe, oder, damit gleichbedeutend, als Gruppe aller birationalen Isomorphismen, des projektiven Raumes $\mathbb{P}_L^{m-1}$, aufgefaßt als projektive Varietät, auf die wir zunächst kurz eingehen.

(11.4) **Satz** *Sei* L *ein Körper und sei* $m \in \mathbb{N}$. *Sei*

$$\chi_L = \chi : PGL(m,L) \to Aut(\mathbb{P}_L^{m-1})$$

die Abbildung, die jedes Element $aL^* = (a_{ij})L^* \in GL(m,L)/L^*$ *auf den Automorphismus*

$$\psi_a : \mathbb{P}_L^{m-1} \longrightarrow \mathbb{P}_L^{m-1},\ (x_0 : ... : x_{m-1}) \mapsto (\Sigma_j a_{0j}x_j : ... : \Sigma_j a_{m-1j}x_j)$$

der projektiven Varietät $\mathbb{P}_L^{m-1}$ *abbildet. Dann gilt*

(a) χ_L *ist ein Homomorphismus von Gruppen*
(b) χ_L *ist injektiv*
(c) χ_L *ist galoisverträglich, d.h. ist* L/K *eine endliche Galoiserweiterung mit der Galoisgruppe* G, *dann gilt*

$$\chi_L(s(aL^*)) = s(\chi_L(aL^*))$$

für alle $a \in GL(m,L)$ *und für alle* $s \in G$.
(d) χ_L *ist surjektiv*

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Die Aussagen (a), (b) und (c) sind leicht zu beweisen. Für Aussage (d) vgl. $[SF]$, Chapter III, exercises 16 & 17. (Ich danke Herrn T. Riedel für den Hinweis auf diese Übungsaufgaben in $[SF]$.)

Aufgrund der verschiedenen galoisverträglichen Deutungen der projektiven linearen Gruppe, nämlich

(a) $PGL(m, L) \cong Aut_L(Mat(m \times m, L))$
(b) $PGL(m, L) \cong$ Gruppe von L-Automorphismen von $L(y_1, ..., y_{m-1})$
(c) $PGL(m, L) \cong Aut(\mathbb{P}_L^{m-1})$,

erhält man mit Hilfe von (11.4) die folgenden Beschreibungen von $H^1(G(L/K), PGL(m, L))$:

(a) Menge aller K-Isomorphieklassen von zentraleinfachen K-Algebren A, so daß $A \otimes_K L \cong Mat(m, L)$
(b) Menge aller K-Isomorphieklassen von Brauerkörpern $F \subset L(y_1, ..., y_{m-1})$
(c) Menge aller K-Isomorphieklassen von über K definierten Brauer-Severi Varietäten, die über L isomorph zu $\mathbb{P}_L^{m-1}$ sind

Dabei ist der Funktionenkörper, der zu der durch Twistung der projektiven Varietät $\mathbb{P}_K^{m-1}$mit einem 1-Kozykel $p : G(L/K) \rightarrow PGL(m, L)$ definierten Brauer-Severi Varietät gehört, K-isomorph zum Brauerkörper F, der durch Twistung von $K(y_1, ..., y_{m-1})$ mit p entsteht; vgl. $[AMT]$, II, 12, Theorem 12.1.

Chatelet hat gezeigt, daß die zu einer zentraleinfachen k-Algebra A gehörende Brauer-Severi Varität genau dann einen k-rationalen Punkt besitzt, wenn A zerfällt, d.h. ähnlich zu einer Matrixalgebra über k ist; vgl. $[C1]$, $[C2]$. Zu diesen Resultaten vgl. man auch die Bemerkungen in $[SE2]$, Chapter III, §1, insbesondere 1.3.

In $[SO]$ wird ein Zusammenhang zwischen Brauerkörpern und Brauer-Severi Varietäten einerseits und gewissen galoistheoretischen Einbettungsproblemen andererseits hergestellt und untersucht.

In $[AM]$ findet man ebenfalls eine Darstellung der Theorie der Brauer-Severi Varietäten. Das Buch $[JA]$ enthält Abschnitte über generische Zerfällungskörper, Brauerkörper und Brauer-Severi Varietäten. Für explizite Gleichungen von Brauer-Severi Varietäten für eine Klasse von Algebren vgl. $[H2]$. Eine ausführliche Darstellung von Zusammenhängen zwischen zentral einfachen Algebren, generischen Zerfällungskörpern und Brauer-Severi Varietäten findet man in $[JN]$ sowie in $[GS]$. Dort findet man jeweils auch eine umfangreiche Literarurliste zu dieser Thematik.

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

Aufgaben und Beispiele

(1) Zeigen Sie, daß der Brauerkörper einer zentraleinfachen Algebra A ein sogenannter generischer Zerfällungskörper von A ist. (Zum Begriff "generischer Zerfällungskörper" und zum Beweis dieser Aussage vgl. $[AMT]$, II, 9, insbesondere Theorem 9.1; oder $[RQ]$, §6. In $[AMT]$ und $[RQ]$ werden weitere Aussagen über den Zusammenhang zwischen zentraleinfachen Algebren und Brauerkörpern bewiesen und vermutet. In $[KRM]$ werden generische Zerfällungskörper in einem wesentlich allgemeineren Rahmen eingeführt und untersucht. E. Witt hat bereits in $[WT3]$ generische Zerfällungskörper von Quaternionenalgebren eingeführt und eine bijektive Korrespondenz zwischen Quaternionenalgebren und Funktionenkörpern vom Geschlecht 0 aufgestellt.)

(2) Zeigen Sie, daß die Brauer-Severi Varietät der Quaternionenalgebra $A_{-1}(a, b)$ durch die Gleichung $az^2 = x^2 - by^2$ gegeben ist (Vgl. $[AMT]$, II, 11, Crollary 11.1, in Verbindung mit II, 12, Theorem 12.1)

Literaturverzeichnis

$[AMT]$ S. Amitsur: Generic splitting fields of central simple algebras, Annals of Math., 62, 1955, 8-43

$[AN]$ J. Kr. Arason: Kohomologische Invarianten quadratischer Formen, J. of Algebra, 36, 1975, 448-491

$[A]$ E. Artin: Galoissche Theorie, Verlag Harri Deutsch, Zürich-Frankfurt, 1966

$[AT]$ E. Artin, J. Tate: Class field theory, Benjamin, New York, 1967

$[AM]$ M. Artin: Brauer-Severi varieties, LNM 917, Springer Verlag, Berlin, 1982, 194-210

$[BA]$ M. I. Bashmakov: The cohomology of Abelian varieties over number fields, Russian Math. Surveys, 27, (2), 1072, 25-70

$[BK]$ N. Bourbaki: Algébre, Hermann, Paris, 1959

$[BF]$ E. Bayer-Fluckiger: Galois cohomology and the trace form, Jahresbericht der Deutschen Mathematiker Vereinigung, 96, 2, 1994, 35-55

$[BP]$ E. Bayer-Fluckiger, R. Parimala: Galois cohomology of classical groups over fields of cohomological dimension ≤ 2, Inventiones Mathematicae, 122, 1995, 195-229

$[C1]$ F. Chatelet: Variations sur un theme de H. Poincare, Ann. Sc. Ecole Normal Superieur, 61, 1944, 249-300

$[C2]$ F. Chatelet: Geometrie diophantine et theorie des algebres, Seminaire Dubreil, expose 17, 1954-1955

$[CH]$ C. Chevalley: The construction and study of an important class of algebras, The Math. Soc. of Japan, 1955

$[DZ]$ A. Delzant: Définition des classes de Stiefel-Whitney d 'un module quadratique sur un corps de caractéristique différente de 2, C.R. Acad. Sci. Paris 255, 1962, 1366-1368

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

[DA] A. Douady: Cohomologie des groupes compact totalement discontinus, Seminaire Bourbaki, Exposé 189, 1959/60, Benjamin, Inc., New York, Amsterdam, 1966

[DK] R. Dedekind: Über die Permutationen des Körpers aller algebraischen Zahlen, Gesammelte Werke, Bd. 2, Braunschweig 1931, 272-292

[D] M. Deuring: Algebren, Zweite, korrigierte Auflage, Springer Verlag, Berlin, 1968

[FR] W. Franz: Topologie I, Allgemeine Topologie, Walter de Gruyter & Co, Berlin, 1968

[GMS] S. Garibaldi, A. Merkurjev, J. P. Serre: Cohomological invariants in Galois cohomology, American Math. Society, Providence R. I., 2003

[GS] P. Gille, T. Szamuely: Central simple algebras and Galois cohomology, Cambridge University Press, 2006

[GI] J. Giraud: Cohomologie non abélienne, Springer Verlag, Berlin 1971

[$G1$] A. Grothendieck: Fondaments de la géométrie algebrique, Extraits du Séminaire Bourbaki, 1957-1962, secretariat mathématiques, Paris, 1962

[$G2$] A. Grothendieck: Technique de descente et théorèmes d'existence en géométrie algébrique. I. Generalitès. Descente par morphismes fidélement plats. Séminaire Bourbaki, 1959-1960, Exposé190

[$G3$] A. Grothendieck: Le groupes de Brauer I, II, III; in "Dix exposés sur la cohomologie des schemás", North Holland, Paris, 1968

[GB] K. Gruenberg: Profinite groups; in: "Algebraic Number Theory", edited by J.W.S. Cassels and A. Fröhlich; Academic Press, New York, 1967

[HB] K. Haberland: Galois cohomology of algebraic number fields, VEB Deutscher Verlag der Wissenschaften, Berlin, 1978; mit einem Anhang von Helmut Koch und einem Anhang von Thomas Zink

[$H1$] F. Henningsen: Algebren und Varietäten, Staatsexamensarbeit, TU Braunschweig, 1996

[$H2$] F. Henningsen: Brauer-Severi-Varietäten und Normrelationen von Symbolalgebren, Dissertation, TU Braunschweig, 2000;
http://www.digibib.tu-bs.de/?docid=00001125

[HS] G.P. Hochschild, J.P. Serre: Cohomology of group extensions, Transactions of the AMS, 74, 1953, 110-134

[H] G.P. Hochschild: Basic constructions in group extension theory, in: Contributions to algebra (Collection of papers dedicated to Ellis Kolchin), Academic Press, New York, 1977; 183-201

[HM] K. Hoechsmann: Zum Einbettungsproblem, JRAM, 229, 81-106, 1968

[JA] N. Jacobson: Finite-dimensional division algebras over fields, Springer Verlag, Berlin, 1996

[JN] J. Jahnel: The Brauer-Severi variety associated with a central simple algebra: A survey, Preprint 52, Linear Algebraic Groups and Related Structures preprint server;
http://www, mathematik.uni-bielefeld.de/LAG/man/o52.html.2000

[J] K. Jänich: Topologie, Springer Verlag, 2-te Auflage, Berlin, 1987

[KT] I. Kersten: Brauergruppen von Körpern, Vieweg, Braunschweig, 1990

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

[KRM] I. Kersten, U. Rehmann: Generic splitting of reductive groups, Tohoku Math. J., 46, 1994, 35-70

[$KMRT$] M.A. Knus, A.S. Merkurjev, M. Rost, J.P. Tignol: The book of involutions, AMS Colloquium Publications, Vol. 44, Providence R I, 1998

[KN] M. Kneser: Lectures on Galois cohomology of the classical groups, Tata Institute lecture notes, Bombay, 1969

[KC] H. Koch: Galoissche Theorie der p-Erweiterungen, Springer Verlag, Berlin, 1970

[KP] H. Koch: Algebraic number fields; in: Number Theory II, Encyclopaedia of Mathematical Sciences, Vol. 62; A. Parshin, I.R. Safarevic (editors); Springer Verlag, Berlin, 1992

[KL] E. Kolchin, S. Lang: Existence of invariant bases, Proceedings AMS, 11, 1960, 140-148

[KR] W. Krull: Galoissche Theorie der unendlichen algebraischen Erweiterungen, Mathematische Annalen, 100, 687-695

[KU] E. Kunz: Algebra, Vieweg Verlag, Braunschweig/Wiesbaden, 1991

[$LG1$] S. Lang: Algebra, Addison Wesley, Reading, 1974

[$LG2$] S. Lang: Rapport sur la cohomologie des groupes, Benjamin, New York, 1966

[$LG3$] S. Lang: Elliptic curves diophantine analysis, Springer Verlag, Berlin, 1978

[$LBVO$] L. Le Bruyn, F. Van Oystaeyen: Brauer groups of fields, Vorlesungen aus dem Fachbereich Mathematik der Universität Essen, Heft 17, 1988

[$LO1$] F. Lorenz: Einführung in die Algebra I, 3-te Auflage, Spektrum Verlag, Heidelberg, 1996

[$LO2$] F. Lorenz: Einführung in die Algebra II, 2-te Auflage, Spektrum Verlag, Heidelberg, 1997

[MAL] S. MacLane: Homology, Springer Verlag, Berlin, 1975

[$MK1$] A. S. Merkurjev: On the norm residue symbol of degree 2, Soviet Math. Doklady, 24, 1981, 546-551

[$MK2$] A. S. Merkurjev: Simple algebras and quadratic forms, Math. U.S.S.R. Izvestiya, 38, 1992, 215-221

[MS] A.S. Merkurjev, A.A. Suslin: K-cohomology of Severi-Brauer varieties and the norm residue homomorphism, Math. U.S.S.R. Izvestiya, 21, 1983, 307-340

[ML] J. Milne: Arithmetic duality theorems, Academic Press, Boston, 1986

[$MN1$] J. Milnor: Introduction to Algebraic K-Theory, Princeton University Press, Princeton, New Jersey, 1971

[$MN2$] J. Milnor: Algebraic K-Theory and quadratic forms, Inventiones Mathematicae, 9, 1969/1970, 318-344

[NK] J. Neukirch: Über das Einbettungsproblem der algebraischen Zahlentheorie, Inventiones Mathematicae, 21, 1977, 59-116

[NSW] J. Neukirch, A. Schmidt, K. Wingberg: Cohomology of number fields, Springer Verlag, Berlin, 2000

[PF] A. Pfister: On the Milnor conjectures: History, Influence, Applications; Jahresbericht der DMV, Band 102, Heft 1, 2000, 15-41

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

[PR] V.P. Platonov, A.S. Rapinchuk: Algebraic groups and number fields, Academic Press, Boston, 1993

[PT] G. Poitou: Cohomologie Galoisienne de modules finis, Dunod, Paris, 1967

[RB] L. Ribes: Introduction to profinite groups and Galois cohomology, Queen's papers in pure math., 24, Kingston, Ontario, 1970

[RQ] P. Roquette: On the Galois cohomology of the projective linear group and its applications to the construction of generic splitting fields of algebras, Mathematische Annalen, 150, 1962, 411-499

[SAH] H. Sah: Automorphisms of finite groups, Journal of Algebra, 10, 1968, 47-68

[SF] I. R. Safarevic: Basic algebraic geometry, Springer Verlag, Berlin, 1974

[$SC1$] W. Scharlau: Quadratische Formen und Galois-Kohomologie, Inventiones Mathematicae, 4, 1967, 238-264

[$SC2$] W. Scharlau: Quadratic and Hermitean forms, Springer Verlag, Berlin, 1985

[SB] H. Schubert: Kategorien I, II, Springer Verlag, Berlin, 1970

[SCH] I. Schur: Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, JRAM, 127, 1904, 20-50 (=Gesammelte Abhandlungen, Band I, Abhandlung 4)

[ST] G. Schwant: Isotropie ternärer quadratischer Formen mit rationalen Koeffizienten, Diplomarbeit, TU Braunschweig, 1995

[$SE1$] J.P. Serre: Local fields, Springer Verlag, New York, 1979

[$SE2$] J.P. Serre: Galois cohomology, Springer Verlag, Berlin, 1997

[$SE3$] J.P. Serre: Topics in Galois theory, Notes written by Henri Darmon, Jones and Bartlett Publishers, Boston, 1992

[$SE4$] J.P. Serre: Modular forms of weight one and Galois representations, in: Algebraic number fields, (A. Fröhlich, ed.), Academic Press, New York, 1977

[$SE5$] J.P. Serre: L'invariant de Witt de la forme $Tr(x^2)$, Commentarii Mathematici Helvetici, 59, 1984, 651-676

[$SGA1$] A. Grothendieck: Revétement etales et groupe fondamental, LNM 224, Springer Verlag, Berlin, 1971

[$SGA4$] Séminaire dé Géométrie Algébrique du Bois Marie, dirigè par M. Artin, A. Grothendieck, J.L. Verdier; Springer Verlag, LNM 269, 270, 1972

[SH] S.S. Shatz: Profinite groups, arithmetic, and geometry, Annals of Mathathematics Studies, 67, Princeton University Press, Princeton, 1972

[SM] J.H. Silverman: The arithmetic of elliptic curves, Springer Verlag, New York, 1986

[SO] J. Sommer: Diophantische Methoden bei der expliziten Lösung von Einbettungsproblemen in der Galoistheorie, Dissertation, TU Braunschweig, 1998; http://www.digibib.tu-bs.de/?docid=00001029

[SP] A. Speiser: Zahlentheoretische Sätze aus der Gruppentheorie, Mathematische Zeitschrift, 5, 1919, 1-6

[SR] T.A. Springer: On the equivalence of quadratic forms, Indagationes Mathematicae, 21, 1959, 241-253

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010

[SW] H.P.F. Swinnerton-Dyer: A brief guide to algebraic number theory, Cambridge University Press, 2001

[$T1$] J. Tate: Duality theorems in Galois cohomology over number fields, Proc. Int. Congress of Math., Stockholm, 1962, 288-295

[$T2$] J. Tate: Cohomology groups of tori in finite Galois extensions of algebraic number fields, Nagoya Math. Journal, 27, 1966, 709-719

[$V1$] V. Voevodsky: Reduced power operations in motivic cohomology, Publ. Math. IHES, 98, 2003, 1-57

[$V2$] V. Voevodsky: Motivic cohomology with $\mathbb{Z}/2$-coefficients, Publ. Math. IHES, 98, 2003, 59-104

[WS] J. S. Wilson: Profinite groups, Clarendon Press, Oxford, 1998

[$WT1$] E. Witt: Theorie der quadratischen Formen in beliebigen Körpern, JRAM, 176, 176, 1937, 31-44

[$WT2$] E. Witt: Schiefkörper über diskret bewerteten Körpern, JRAM, 176, 1936, 153-156

[$WT3$] E. Witt: Über ein Gegenbeispiel zum Normensatz, Mathematische Zeitschrift, 39, 1934, 12-28

Typeset with Scientific Word 3.0 and AMS LaTex

http://www.digibib.tu-bs.de/?docid=00032723 19/03/2010